

GUTRIDE SAFIER LLP

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

Kali R. Backer (State Bar No. 342492)

kali@gutridesafier.com

Anthony J. Patek (State Bar No. 228964)

anthony@gutridesafier.com

100 Pine Street, Suite 1250

San Francisco, CA 94111

Telephone: (415) 639-9090

Facsimile: (415) 449-6469

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

VISHAL SHAH, JONATHAN GABRIELLI,
and CHRISTINE Q. WILEY, as individuals,
on behalf of themselves, the general public,
and those similarly situated,

Plaintiffs,

v.

HILTON WORLDWIDE HOLDINGS INC.,

Defendant.

CASE NO. 5:2025-cv-01018-EKL

**AMENDED CLASS ACTION
COMPLAINT FOR INVASION OF
PRIVACY; INTRUSION UPON
SECLUSION; WIRETAPPING IN
VIOLATION OF THE CALIFORNIA
INVASION OF PRIVACY ACT
(CALIFORNIA PENAL CODE § 631);
USE OF A PEN REGISTER IN
VIOLATION OF THE CALIFORNIA
INVASION OF PRIVACY ACT
(CALIFORNIA PENAL CODE § 638.51);
COMMON LAW FRAUD, DECEIT
AND/OR MISREPRESENTATION;
UNJUST ENRICHMENT; BREACH OF
CONTRACT; BREACH OF IMPLIED
COVENANT OF GOOD FAITH AND
FAIR DEALING; AND TRESPASS TO
CHATTELS**

JURY TRIAL DEMANDED

TABLE OF CONTENTS

1	INTRODUCTION	4
2	THE PARTIES.....	5
3	JURISDICTION AND VENUE	6
4	SUBSTANTIVE ALLEGATIONS	7
5	A. Defendant Owns and Operates Hilton.com for the Express Purpose of Marketing	
6	and Leasing Hilton-Owned and Hilton-Affiliated Hotels.....	7
7	B. Defendant Purposefully Directs Activity Into California and Avails Itself of	
8	California Law and the California Market.....	11
9	C. Defendant Programmed the Website to Include Third-Party Resources that Utilize	
10	Cookie Trackers.	15
11	D. Defendant Falsely Informed Users That They Could Opt Out of the Website’s Use	
12	of Cookies.	20
13	E. Defendant’s Conduct Violated Its Own Privacy Statement.....	25
14	F. The Private Communications Collected As a Result of Third Party Cookies	
15	Transmitted When Visiting Defendant’s Website.	25
16	1. Google Cookies.....	25
17	2. Adobe Cookies.....	30
18	3. Additional Cookies	36
19	G. The Private Communications Collected are Valuable.....	39
20	PLAINTIFFS’ EXPERIENCES	40
21	HILTON’S KNOWLEDGE AND INTENT TO AID THIRD PARTIES.....	49
22	TOLLING	50
23	CLASS ALLEGATIONS	51
24	CAUSES OF ACTION	53
25	First Cause of Action: Invasion of Privacy.....	53
26	Second Cause of Action: Intrusion Upon Seclusion.....	56
27	Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy	
28	Act (California Penal Code § 631).....	58
	Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of	
	Privacy Act (California Penal Code § 638.51)	62

1 Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation..... 64

2 Sixth Cause of Action: Unjust Enrichment..... 66

3 Seventh Cause of Action: Breach of Contract 68

4 Eighth Cause of Action: Breach of Implied Covenant of Good Faith and Fair Dealing.. 69

5 Ninth Cause of Action: Trespass to Chattels 71

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

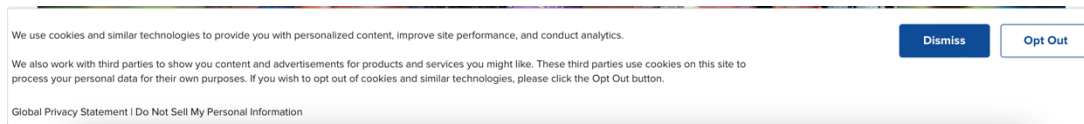
27

28

1 Plaintiffs Vishal Shah, Jonathan Gabrielli, and Christine Wiley (“Plaintiffs”) bring this
 2 action on behalf of themselves, the general public, and all others similarly situated against Hilton
 3 Worldwide Holdings Inc. (“Defendant” or “Hilton”). Plaintiffs’ allegations against Defendant
 4 are based upon information and belief and upon investigation of Plaintiffs’ counsel, except for
 5 allegations specifically pertaining to Plaintiffs, which are based upon Plaintiffs’ personal
 6 knowledge. Plaintiffs file this Amended Complaint pursuant to the Court’s June 11, 2025 Order.
 7 (ECF 30.)

8 INTRODUCTION

9 1. This Amended Class Action Complaint concerns an egregious privacy violation
 10 and total breach of consumer trust in violation of California law. When California consumers
 11 visit Defendant’s website (www.hilton.com, the “Website”), Defendant displays to them a popup
 12 cookie consent banner. Defendant’s cookie banner discloses that the Website uses cookies but
 13 expressly gives users the option to control how they are tracked and how their personal data is
 14 used. Defendant assures visitors that they can choose to “Opt Out” of cookies as shown in the
 15 following screenshot:



16
 17
 18 2. Like most websites, Defendant designed the Website to include resources and
 19 programming scripts from third parties that enable those parties to place cookies and other
 20 similar tracking technologies on visitors’ browsers and devices and to transmit cookies along
 21 with user data. However, unlike other websites, Defendant’s Website offers consumers a choice
 22 to browse without being tracked, followed, and targeted by third party data brokers and
 23 advertisers. However, Defendant’s promises are outright lies, designed to lull users into a false
 24 sense of security. Even after users elect to “Opt Out” of cookies, Defendant surreptitiously
 25 enables several third parties – including Google LLC (DoubleClick), Adobe Inc. (Adobe
 26 Marketing Cloud and Adobe Audience Manager), Microsoft, Inc. (Bing), Snap, Inc., *and more*
 27
 28

(the “Third Parties”) – to place and/or transmit cookies that track users’ website browsing activities and eavesdrop on users’ private communications on the Website.

3. Contrary to their express opt out or rejection of cookies and tracking technologies on the Website, Defendant nonetheless caused cookies, including the Third Parties’ cookies, to be sent to Plaintiffs’ and other visitors’ browsers, stored on their devices, and transmitted to the Third Parties along with user data. These third-party cookies permitted the Third Parties to track and collect data in real time regarding Website visitors’ behaviors and communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.

4. The Third Parties analyze and aggregate this user data across websites and time for their own purposes and financial gain, including, creating consumer profiles containing detailed information about a consumer’s behavior, preferences, and demographics; creating audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and performing targeted advertising and marketing analytics. Further, the Third Parties share user data and/or user profiles to unknown parties to further their financial gain.

5. This type of tracking and data sharing is exactly what the Website visitors who clicked or selected the “Opt Out” button on the Website’s cookie consent banner sought to avoid. Defendant falsely told Website users that it respected their privacy and that they could avoid tracking and data sharing when they browsed the Website. Despite receiving notice of consumers’ express declination of consent, Defendant defied it and violated state statutes, tort duties, and also breached its contractual duties and the implied covenant of good faith and fair dealing with Plaintiffs and those similarly situated Website users.

THE PARTIES

6. Plaintiff Vishal Shah is, and was at all relevant times, an individual and resident of San Jose, California. Plaintiff intends to remain in California and makes his permanent home there

1 7. Plaintiff Jonathan Gabrielli is, and was at all relevant times, an individual and
2 resident of Oakland, California. Plaintiff intends to remain in California and makes his
3 permanent home there.

4 8. Plaintiff Christine Wiley is, and was at all relevant times, an individual and
5 resident of Long Beach, California. Plaintiff intends to remain in California and makes his
6 permanent home there.

7 9. Defendant Hilton Worldwide Holdings Inc. is a Delaware corporation with its
8 headquarters and principal place of business in McLean, Virginia.

9 **JURISDICTION AND VENUE**

10 10. This Court has jurisdiction over the subject matter of this action pursuant to 28
11 U.S.C. § 1332(d)(2). The aggregate amount in controversy exceeds \$5,000,000, exclusive of
12 interest and costs; and Plaintiffs and Defendant are citizens of different states.

13 11. The injuries, damages and/or harm upon which this action is based, occurred or
14 arose out of activities engaged in by Defendant within, affecting, and emanating from, the State
15 of California. Defendant regularly conducts and/or solicits business in, engages in other
16 persistent courses of conduct in, and/or derives substantial revenue from products and services
17 provided to persons in the State of California. Defendant has engaged, and continues to engage,
18 in substantial and continuous business practices in the State of California.

19 12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a
20 substantial part of the events or omissions giving rise to the claims occurred in the state of
21 California, including within this District.

22 13. Plaintiffs accordingly allege that jurisdiction and venue are proper in this Court.
23
24
25
26
27
28

SUBSTANTIVE ALLEGATIONS

A. Defendant Owns and Operates Hilton.com for the Express Purpose of Marketing and Leasing Hilton-Owned and Hilton-Affiliated Hotels

14. Defendant is a globally recognized hospitality company and one of the largest and most well-known hotel chains in the world. Defendant operates a wide range of hotels and resorts under various brands, catering to different customer segments and needs.

15. Defendant's 10-K for the year 2023 states that "'Hilton,' 'the Company,' 'we,' 'us' and 'our' refer to Hilton Worldwide Holdings Inc., together with all of its consolidated subsidiaries. Except where the context requires otherwise, references to our 'properties' refer to the hotels, resorts and timeshare properties that are managed, franchised, owned or leased by us"

16. Hilton's 10-K for 2023 also states that "Hilton is one of the largest hospitality companies in the world, with 7,530 properties comprising 1,182,937 rooms in 126 countries and territories as of December 31, 2023."

17. In its 2023 10-K, Hilton reiterates that it "operates" its hotels through both direct and indirect means:

We operate our business through: (i) a management and franchise segment and (ii) an ownership segment, each of which is reported as a segment based on (a) delivering a similar set of products and services and (b) being managed separately given its distinct economic characteristics. The management and franchise segment includes all of the hotels we manage for third-party owners, as well as all franchised hotels that license our intellectual property ("IP"), including our brand names, trademarks and service marks, and to which we provide other contracted services, but the day-to-day services of the hotels are operated or managed by someone other than us. Revenues from this segment include: (i) management and franchise fees charged to third-party hotel owners; (ii) licensing fees from our strategic partners, including co-branded credit card providers, and HGV; and (iii) fees for managing hotels in our ownership segment. The ownership segment primarily derives revenues from nightly hotel room sales, food and beverage sales and other services at our consolidated owned and leased hotels. For more information regarding our segments, refer to "—Our Business—Management and Franchise" and "—Our Business—Ownership" below.

1 18. Thus, while Hilton says that the “day-to-day” services may be handled by
2 “someone else,” Hilton holds itself out as the ultimate owner and operator of Hilton-branded
3 hotels, although it may do so through franchisees, partners, and related Hilton subsidiaries.

4 19. Based on Hilton’s above statements, Plaintiffs allege that, even where a Hilton
5 subsidiary is involved, Hilton’s public filings indicate that it maintains substantial control over
6 hotels.

7 20. In its 2024 earnings call, Hilton’s CEO has stated that “Approximately half of our
8 pipeline is under construction, and we continue to have more rooms under construction than any
9 other hotel company, accounting for more than 20% of industry share and nearly 4x our existing
10 share of supply. We’ve seen tremendous interest from owners through our exclusive agreement
11 with small luxury hotels of the world, with the pace of initial property sign-ups far exceeding
12 our expectations.”

13 21. The CEO states in the same call that “Under our strategic partnership, we added
14 nearly 300 boutique luxury properties to our system in July, with an additional 100 properties
15 expected to join later this year. Adding these unique properties to our network is highly
16 complementary to our existing luxury portfolio and significantly increases our luxury offerings
17 for guests around the world without any capital commitment.”

18 22. Again, the above statements represent Hilton as the owner and operator of the
19 Hilton hotel network, even where the network includes strategic partners.

20 23. News outlets report new Hilton hotels being built in California regularly,
21 particularly through the period of 2023 to the present. Such reports include:

- 22 • A new Tempo by Hilton in San Diego in 2025. See [https://stories.hilton.com/growth-](https://stories.hilton.com/growth-development/new-hilton-openings-in-2025)
23 development/new-hilton-openings-in-2025.
- 24 • A Hilton Garden Inn in Merced in 2024. Merced Sun-Star.
25 <https://www.mercedsunstar.com/news/local/article290481614.html>
- 26 • A Hilton in Universal City, CA in 2024. [https://www.latimes.com/business/story/2024-](https://www.latimes.com/business/story/2024-09-18/universal-city-hotel-expansion-project-clears-early-approval-hurdle)
27 09-18/universal-city-hotel-expansion-project-clears-early-approval-hurdle

- 1 • An Irvine Hilton in 2023. [https://www.constructiondive.com/news/rd-olson-start-](https://www.constructiondive.com/news/rd-olson-start-construction-arcadia-california-hotel-hilton/687844/)
- 2 [construction-arcadia-california-hotel-hilton/687844/](https://www.constructiondive.com/news/rd-olson-start-construction-arcadia-california-hotel-hilton/687844/)
- 3 • A new Hilton “Tapestry” brand hotel in Napa. Managed by partner, but owned and
- 4 operated by/for Hilton. [https://www.hoteldive.com/news/knoll-napa-valley-tapestry-](https://www.hoteldive.com/news/knoll-napa-valley-tapestry-hilton-opening/711606/)
- 5 [hilton-opening/711606/](https://www.hoteldive.com/news/knoll-napa-valley-tapestry-hilton-opening/711606/).

6 24. The news release for the Hilton Tapestry hotel in Napa, California, included a
 7 comment from Hilton Worldwide Inc. CEO Christopher Nassetta, regarding growth of “full-
 8 service and collection brands” such as Tapestry, which confirms that Defendant Hilton is directly
 9 involved in the California-specific building activities reported above.

10 25. Defendant Hilton owns and operates the Hilton.com website. The Website lists
 11 Hilton Worldwide Holdings, Inc. as its owner.

12 26. The Website is an interactive platform that allows people throughout the United
 13 States, and California in particular, to browse Hilton-owned and affiliated properties and lease
 14 them. At least one of the servers on which Hilton runs the website are located in Santa Clara,
 15 California, with an IP address of 23.40.24.118.

16 27. The Website allows visitors to receive information about hotels in California and
 17 make hotel reservations in California.

18 28. Hilton states in its 10-K that “[w]e use our website at stories.hilton.com, our
 19 Facebook page at facebook.com/hiltonnewsroom and our corporate X (formerly Twitter)
 20 account at twitter.com/hiltonnewsroom as channels of distribution of company information.”

21 29. Hilton highlights the Website in its annual report as a key factor in its revenues,
 22 and thus a potential vulnerability to its business operations:

23 Failures in, material damage to or interruptions in our information
 24 technology systems, software or websites, including as a result of
 25 cyber-attacks on our systems or systems operated by third parties
 26 that provide operational and technical services to us, costs
 27 associated with protecting the integrity and security of personal data
 28 and other sensitive information and difficulties in updating our
 existing software or developing or implementing new software
 could have a material adverse effect on our business or results of
 operations”

30. Hilton's 10-K also identifies the growth of reservation systems that compete with the Hilton.com Website as something that "could adversely affect our business and profitability."

31. Hilton's 10-K goes on to say that acquiring reservations through its Website rather than third party reservation systems is important both as a means of limiting fees and fostering brand loyalty:

The growth of internet reservation channels could adversely affect our business and profitability. A significant percentage of hotel rooms for individual guests are booked through internet travel intermediaries, to whom we commit to pay various commissions and transaction fees for sales of our rooms through their systems. Search engines and peer-to-peer inventory sources also provide online travel services that compete with our business. If these bookings increase, these hospitality intermediaries may be able to obtain higher commissions or other significant concessions from us or our franchisees. These hospitality intermediaries also may reduce bookings at our hotel properties by de-ranking our hotels in search results on their platforms, and other online providers may divert business away from our hotels. Although our contracts with many hospitality intermediaries limit transaction fees for hotels, there can be no assurance that we will be able to renegotiate these contracts upon their expiration with terms as favorable as the provisions that existed before the expiration, replacement or renegotiation. Moreover, hospitality intermediaries generally employ aggressive marketing strategies, including expending significant resources for online and television advertising campaigns to drive consumers to their websites. As a result, consumers may develop brand loyalties to the intermediaries' brands, websites and reservations systems rather than to the Hilton brands and systems. If this happens, our business and profitability may be significantly affected over time as shifting customer loyalties divert bookings away from our websites, which increases costs to hotels in our system. Internet travel intermediaries also have been subject to regulatory scrutiny, particularly in Europe. The outcome of this regulatory activity may affect our ability to compete for direct bookings through our own internet channels.

32. Hilton's 10-K explicitly identifies the Website as "an important component of our business operations":

Our reservation system is an important component of our business operations and a disruption to its functioning could have an adverse effect on our performance and results. We manage a

global reservation system that communicates reservations to our branded hotels when made by individuals directly, either online, by telephone to our call centers, through devices via our mobile application, or through intermediaries like travel agents, internet travel websites and other distribution channels. The cost, speed, efficacy and efficiency of the reservation system are important aspects of our business and are important considerations of hotel owners in choosing to affiliate with our brands. Any disruption to the continuity of our reservation system, including any failure to maintain or upgrade such system, may adversely affect our ability to serve customers effectively and support reservations at our hotels.

(Emphasis added.) On information and belief, the Website is integrated with the “reservation system” that Hilton uses to communicate reservations to “our branded hotels.”

33. Hilton uses its Website to facilitate online sales of hotel rooms for its subsidiaries and partners, including subsidiaries and partners in California. Its partners and subsidiaries use the Website to provide Hilton (and by extension, consumers) with their hotel offerings, prices, options, and other business information. When a reservation is made, Hilton collects and validates the visitor’s payment, and processes the payment in conjunction with third party payment processors. As part of this process, Hilton collects and stores personal information for the room purchasers, including purchasers in California.

34. Hilton also utilizes third parties to collect and track information regarding visitors to the Website, as described further below in the section titled Defendant Programmed the Website to Include Third-Party Resources that Utilize Cookie Trackers.

B. Defendant Purposefully Directs Activity Into California and Avails Itself of California Law and the California Market

35. California represents roughly 10% of the U.S. population and about 15% of its gross domestic product. It is thus a desirable market for any company operating in the United States.

36. Hilton’s 10-K notes that compliance with various regulations and laws that limit ability to transfer data—particularly California state law—affects its ability to do business and “acquire new customers”:

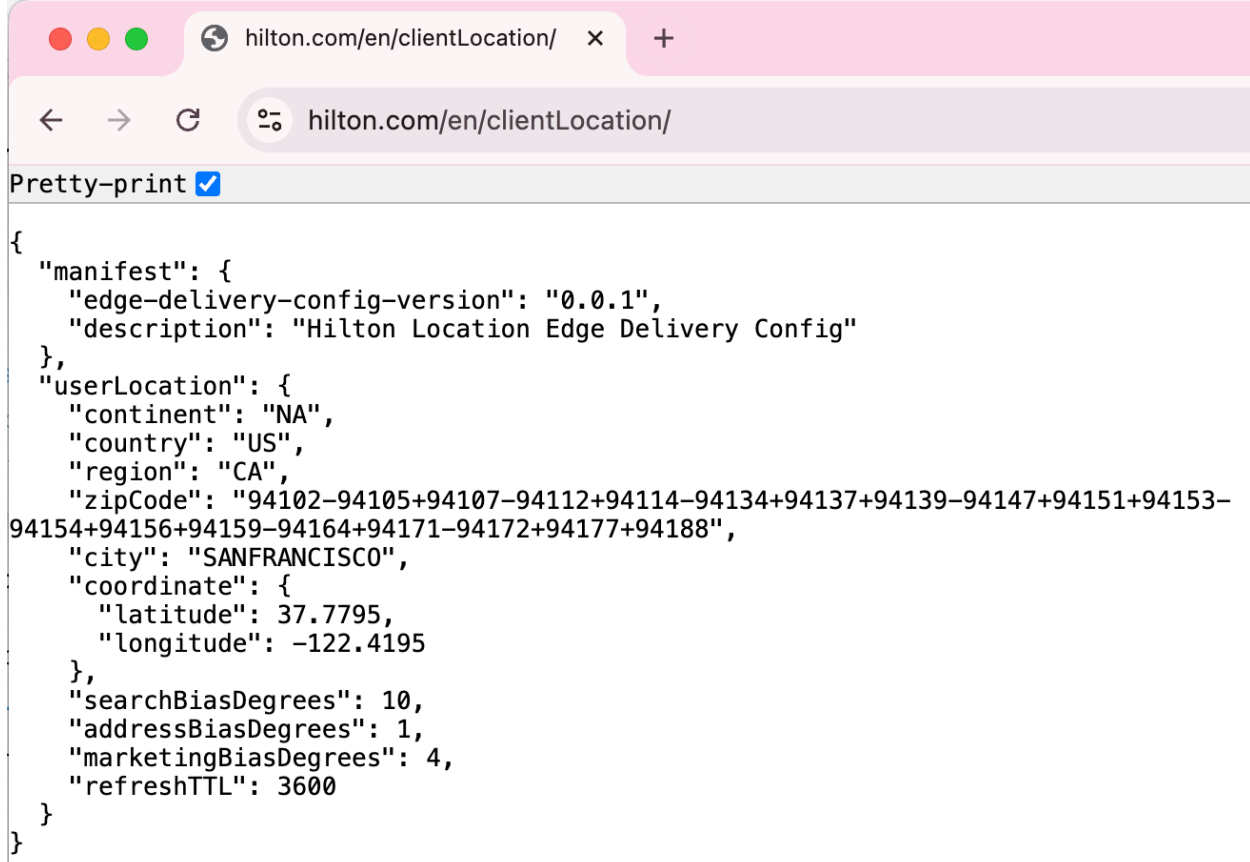
We rely on a variety of direct marketing techniques, including telemarketing, email and social media marketing and postal mailings, and we are subject to various laws and regulations in the U.S. and internationally that govern marketing and advertising practices. Any further restrictions in laws and court or agency interpretations of such laws, such as the Telephone Consumer Protection Act of 1991, the Telemarketing Sales Rule, the CAN-SPAM Act of 2003, *various U.S. state laws, such as the California Privacy Rights Act*, international data protection laws, such as the E.U. General Data Protection Regulation ("GDPR"), *and laws limiting the cross-border transfer of data that govern these activities* or new laws that become effective in the future *could adversely affect current or planned marketing activities* and cause us to change our marketing strategy. *If this occurs, we may not be able to develop adequate alternative marketing strategies, which could affect our ability to maintain relationships with our customers and acquire new customers.*")

(Emphasis added.). This demonstrates that Hilton operates in California and avails itself of California law, by virtue of the recognition that it must comply with state laws "such as the California Privacy Rights Act." It also shows that its Website is an important marketing tool for its operations in California, including the collection of data that results from the Website.

37. Accordingly, Defendant has modified its Website specifically to take advantage of the California market.

38. Specifically, Defendant has implemented code in its Website that geolocates each visitor, and particularly those visiting the Website from a location in California.

39. When a user browses the Hilton website, Defendant causes the user's browser to execute code that performs an HTTP GET call to <https://www.hilton.com/en/clientLocation/>. In the process of making that call, the user's browser transmits the user's IP address to the Hilton website. An application on the Hilton Website — which Hilton has entitled "Hilton Location Edge Delivery Config" — then determines the user's latitude and longitude, city, state, and zip code:



40. Thus, Defendant knows when a Website visitor is located in California, and causes cookies to be placed on the user's device that remain on the device and allow third parties to collect and amass data regarding the California user's online activity. Hilton uses third party cookies and tracking technology to track and collected browsing data from California consumers. Hilton uses this information to target ads to these consumers, "maintain relationships" with customers, and "acquire new customers" as described above.

41. Defendant relies on such information in its marketing strategy to "maintain relationships" with customers and "acquire new customers."

42. If the visitor is located in California, Defendant's code follows a script that presents a California-specific notice to California visitors, as described above in paragraph 1 and further below. Hilton's Privacy Policy explicitly states that this action is specific to IP addresses within California:

If you would like to opt out of the sale of your personal information, you may do so by clicking on the banner that appears on any Hilton website when you access

1 *that site from an IP address that relates to California* or by visiting our website at
2 datarights.hilton.com or click the “Personal Data Requests” link at the bottom of
3 any Hilton website to submit your request. Please note that when you opt out of
4 cookies, tags, and pixels, that opt out only pertains to the device and the browser
that you are using when you opt out. If you wish to opt out for other devices or
browsers, you must opt out again when you are using those devices or browsers.

5 (Emphasis added). (N.B., subsequent to filing of this lawsuit, Hilton still allows placement of
6 third party tracking cookies, but has turned off the notice to California consumers that they can
7 opt-out of the tracking under California law.)

8 43. Hilton thus targets California consumers to extract, collect, maintain, distribute,
9 and exploit for its own profit, not only the California consumers’ payment information that it
10 diverts to its own servers, but also all of the other personal identifying information that it extracts
11 from the software it permanently installs on their devices without their knowledge or consent

12 44. The information used includes information collected surreptitiously, without
13 consent, and in contradiction to its promises not to do so for those California visitors who
14 decline use of third party cookies.

15 45. Accordingly, through those business activities, Hilton tortiously violated
16 consumers’ privacy through its collection, maintenance, and sharing of valuable personal data
17 from California consumers. It is also possible that Hilton sold such information in violation of
18 its promise not to do so.

19 46. Each of Hilton’s actions above was undertaken in its regular course of business
20 and is an intentional act. For example, the coding of its Website, its inclusion of third party
21 cookies, and the tracking that subsequently occurred are all results of acts that Hilton
22 intentionally performed.

23 47. Hilton knows that the unconsented tracking will harm California consumers.
24 Indeed, the fact that it included the California privacy notices and putative “opt-out”
25 mechanisms are designed to alleviate the concern that California consumers will suffer harm
26 by using Defendant’s website. Because Hilton’s actions are a “but-for” cause of the Third
27 Parties’ ability to perform the unconsented tracking via cookies, and because Hilton knew that
28

1 failure to implement the protections it was advertising and agreeing to would harm California
 2 consumers, it knew its actions would harm California consumers. Moreover, because the
 3 notices and promises are California-specific, Hilton's tortious and contracting activities at issue
 4 are expressly aimed at California, and no other state. To the best of Plaintiffs' knowledge,
 5 Hilton still has not corrected the privacy violations noted above, other than to turn off the
 6 banner that told people they could turn off use of non-essential cookies.

7 48. Hilton thus expressly aims its Website activities into California. All of the
 8 above actions are Hilton's own choices, and not random or fortuitous activities. It implements
 9 the code that calls the cookies that were placed on Plaintiffs' and other visitors' computers. It
 10 chooses to reach into California specifically in order to access the California market, as
 11 demonstrated by its California-specific Website coding.

12 49. All of Plaintiffs' claims, described in further detail below, arise from or relate to
 13 Hilton's conduct in California. The claims all arise from tortious behavior or breach of
 14 contract that arises from Hilton's practice of promising to California consumers that it would
 15 not track their data if they turned off such tracking, and its subsequent violation of that
 16 promise.

17
 18 **C. Defendant Programmed the Website to Include Third-Party Resources that**
 19 **Utilize Cookie Trackers.**

20 50. Every website, including the Website, is hosted by a server that sends and
 21 receives communications in the form of HTTP requests, such as "GET" or "POST" requests, to
 22 and from Internet users' browsers. For example, when a user clicks on a hyperlink on the
 23 Website, the user's browser sends a "GET" request to the Website's server. The GET request
 24 tells the Website server what information is being requested (e.g., the URL of the webpage being
 25 requested) and instructs the Website's server to send the information back to the user (e.g., the
 26 content of the webpage being requested). When the Website server receives an HTTP request, it
 27 processes that request and sends back an HTTP response. The HTTP request includes the client's
 28 IP address so that the Website server to knows where to send the HTTP response.

1 51. An IP address (Internet Protocol address) is a unique numerical label assigned to
2 each device connected to a network that uses the Internet Protocol for communication, typically
3 expressed as four sets of numbers separated by periods (e.g., 192.168.123.132 for IPv4
4 addresses). IP addresses can identify the network a device is on and the specific device within
5 that network. Public IP addresses used for internet-facing devices reveal geographical locations,
6 such as country, city, or region, through IP geolocation databases.

7 52. Defendant voluntarily integrated “third-party resources” from the Third Parties
8 into its Website programming. “Third-party resources” refer to tools, content or services
9 provided by third-parties, such as analytics tools, advertising networks, or payment processors,
10 that a website developer utilizes by embedding scripts, styles, media, or application
11 programming interface (API) into the website’s code. Defendant’s use of the third-party
12 resources on the Website is done so pursuant to agreements between Defendant and those Third
13 Parties.

14 53. The Website causes users’ devices to store and/or transmit both first-party and
15 third-party tracking cookies. Cookies are small text files sent by a website server to a user’s web
16 browser and stored locally on the user’s device. As described below, cookies generally contain
17 a unique identifier which enables the website to recognize and differentiate individual users.
18 Cookie files are sent back to the website server along with HTTP requests, enabling the website
19 to identify the device making the requests, and to record a session showing how the user interacts
20 with the website.

21 54. First-party cookies are those that are placed on the user’s device directly by the
22 web server with which the user is knowingly communicating (in this case, the Website’s server).
23 First-party cookies are used to track users when they repeatedly visit the same website.

24 55. A third-party cookie is set by a third-party domain/webserver (e.g.,
25 www.google.com; doubleclick.net; bing.com; tr.snapchat.com; etc.). When the user’s browser
26 loads a webpage (such as a webpage of the Website) containing embedded third-party resources,
27 the third-parties’ programming scripts typically determine whether the third-party cookies are
28

1 already stored on the user's device and cause the user's browser to store those cookies on the
2 device if they do not yet exist. Third-party cookies include an identifier that allows the third-
3 party to recognize and differentiate individual users across websites (including the Website) and
4 across multiple browsing sessions.

5 56. As described further below, the third-party cookies stored on and/or loaded from
6 users' devices when they interact with the Website are transmitted to those third parties, enabling
7 them to surreptitiously track in real time and collect Website users' personal information, such
8 as their browsing activities and private communications with Defendant, including the following:

- 9 • **Browsing History:** Information about the webpages a Website user visits,
10 including the URLs, titles, and keywords associated with the webpages viewed,
11 time spent on each page, and navigation patterns;
- 12 • **Visit History:** Information about the frequency and total number of visits to the
13 Website;
- 14 • **Website Interactions:** Data on which links, buttons, or ads on the Website that
15 a user clicks;
- 16 • **User Input Data:** The information the user entered into the Website's form fields
17 and/or search interface, including search queries, dates of visits, number of
18 people, the user's name, age, gender, email address, location, location preferences
19 within a city, and/or payment information;
- 20 • **Demographic Information:** Inferences about age, gender, and location based on
21 browsing habits and interactions with Website content;
- 22 • **Interests and Preferences:** Insights into user interests based on the types of
23 Website content viewed, products searched for, or topics engaged with;
- 24 • **Shopping Behavior:** Information about the Website products viewed or added to
25 shopping carts;
- 26 • **Device Information:** Details about the Website user's device, such as the type of
27 device (mobile, tablet, desktop), operating system, and browser type;

- 1 • **Referring URL:** Information about the website that referred the user to the
- 2 Website;
- 3 • **Session Information:** Details about the user’s current Website browsing session,
- 4 including the exact date and time of the user’s session, the session duration and
- 5 actions taken on the Website during that session;
- 6 • **User Identifiers:** A unique ID that is used to recognize and track a specific
- 7 Website user across different websites over time; and/or
- 8 • **Geolocation Data:** General location information based on the Website user’s IP
- 9 address or GPS data, if accessible.

10 (Collectively, the browsing activities and private communications listed in the bullet points
11 above shall be referred to herein as “Private Communications”).

12 57. Third-party cookies can be used for a variety of purposes, including (i) analytics
13 (e.g., tracking and analyzing visitor behavior, user engagement, and effectiveness of marketing
14 campaigns); (ii) personalization (e.g., remembering a user’s browsing history and purchase
15 preferences to enable product recommendations); (iii) advertising/targeting (e.g., delivering
16 targeted advertisements based on the user’s consumer profile (i.e., an aggregated profile of the
17 user’s behavior, preferences, and demographics); and (iv) social media integration (e.g., enabling
18 sharing of users’ activities with social media platforms). Ultimately, third-party cookies are
19 utilized to boost website performance and revenue through the collection, utilization, and
20 dissemination of user data.

21 58. As they interact with the Website (e.g., by entering data into forms, clicking on
22 links, and making selections), Website users communicate Private Communications to
23 Defendant, including their browsing history, visit history, website interactions, user input data,
24 demographic information, interests and preferences, shopping behaviors, device information,
25 referring URLs, session information, user identifiers, and/or geolocation data.

26 59. Defendant chose to install or integrate its Website with resources from the Third
27 Parties that, among other things, use cookies. Thus, when consumers visit the Website, both
28

1 first-party cookies and third-party cookies are placed on their devices and/or transmitted. This is
2 caused by software code that Defendant incorporates into its Website, or that Defendant causes
3 to be loaded. Because Defendant controls the software code of its Website, it has complete
4 control over whether first-party and third-party cookies are placed on its users' devices and/or
5 transmitted to third parties.

6 60. Defendant explained the third-party cookies it used on the Website as follows in
7 its Privacy Statement:

8 [We have collected the following categories of personal information in the past 12
9 months:]

10 Internet or other electronic network activity information, including information
11 regarding a customer's interaction with Hilton websites, applications, or
advertisements

12 [We have obtained this personal information from the following sources:]

13 Directly from consumers themselves via cookies, server logs, web beacons, tags,
14 pixels, and other similar technologies

15 [We collected this personal information for the following business or commercial
16 purposes:]

- 17 • Perform analytics in order to provide guests with personalized offers and
content
- 18 • Perform analytics to improve business operations
- 19 • Marketing
- 20 • Share that data with advertising networks who serve personalized
advertisements
- 21 • Detect and prevent fraud

22 [We have shared this personal information with the following categories of third
parties:]

- 23 • Advertising networks
- 24 • Analytics providers for our websites and mobile applications

25 ...

26 We partner with certain third-party service providers to collect information to
27 engage in analytics, auditing, research, and reporting. These third parties may use
server logs, web beacons, tags, pixels, and similar technologies, and they may set
28 and access cookies on your computer or other device.

...

We also partner with third parties to provide advertising services that are targeted based on your online activities across websites, mobile apps, and devices over time (commonly referred to as “interest-based advertising”). Our advertising partners may collect information about your activities on our Services on your current device and combine it with information about your activities on other websites, mobile apps, and devices. They may collect such information using server logs, cookies, web beacons, tags, pixels, mobile advertising IDs (such as Facebook cookies or Google’s Advertising ID), cross-device linking, and similar technologies. For example, our advertising partners may use the fact that you visited our website to target advertising to you on other websites and mobile apps on your current device or on other devices you use. They may match your browsers or devices if you log into the same online service on multiple devices or if your devices share similar attributes that support an inference that they are used by the same person or household. This means that information about your activity on websites or apps on your current browser or device may be combined and used with information collected from your other browsers or devices.

...

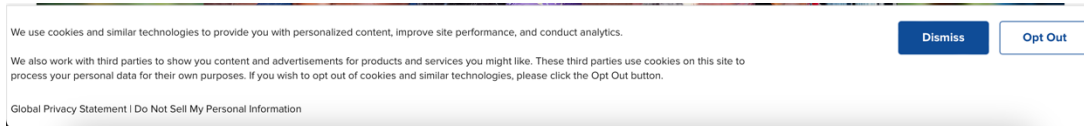
We also cooperate with third parties to serve targeted advertising based on your online activities across different websites, mobile applications, and devices over time. Our advertising partners may collect information about your activities related to our services on your current device and combine it with information about your activities on other websites, mobile applications, and devices. They may collect this information using server logs, cookies, web beacons, tags, pixels, mobile advertising IDs, cross-device linking and similar technologies. This may include your personal information.¹

D. Defendant Falsely Informed Users That They Could Opt Out of the Website’s Use of Cookies.

61. When consumers in California visited the Website, the Website immediately displayed to them a popup cookie consent banner. As shown in the screenshot below, the cookie consent banner stated, “We use cookies and similar technologies to provide you with personalized content, improve site performance, and conduct analytics. We also work with third parties to show you content and advertisements for products and services you might like. These third parties use cookies on this site to process your personal data for their own purposes. If you

¹ Hilton’s Global Privacy Statement (Last Updated: May 10, 2023) (available at <https://web.archive.org/web/20231002094700/https://www.hilton.com/en/p/global-privacy-statement/>) (the “Privacy Statement”). Defendant has subsequently updated its Privacy Statement but, based on information and belief, this version was in effect at the time that Plaintiffs opted out of cookies on the Website.

wish to opt out of cookies and similar technologies, please click the Opt Out button.” The banner then purported to provide users the opportunity to select an “Opt Out” of cookies button as shown in the following screenshot from the Website:



62. Website users who clicked or selected the “Opt Out” button, indicating their choice and/or agreement to opt out of or reject all cookies and tracking technologies in use on the Website, could then continue to browse the Website, and the popup cookie consent banner disappeared.

63. Defendant’s popup cookie consent banner led Plaintiffs, and all those Website users similarly situated, to believe that they opted out of or rejected all cookies and tracking technologies, especially those that used to “personalize[] content, improve site performance, and conduct analytics” and those that allow third parties to “process your personal data for their own purposes.” The banner further reasonably led Plaintiffs and those Website users similarly situated to believe that Defendant would not allow third parties, through cookies, to access their Private Communications with the Website, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, upon clicking or selecting the “Opt Out” button.

64. Defendant’s representations, however, were false. In truth, Defendant did not abide by its users’ wishes. When users selected the “Opt Out” button, they provided notice to Defendant that they did not consent to the placement or transmission of third-party cookies that would allow those parties to obtain their Private Communications with the Website. Nevertheless, Defendant caused the Third Party tracking cookies to be placed on Website users’ browsers and devices and/or transmitted to the Third Parties along with user data.

65. In particular, when users clicked or selected the “Opt Out” button, Defendant nonetheless continued to cause the Third Parties’ cookies to be placed on users’ devices and/or

1 transmitted to the Third Parties along with user data, enabling them to collect user data in real
2 time that discloses Website visitors' Private Communications, including browsing history, visit
3 history, website interactions, user input data, demographic information, interests and
4 preferences, shopping behaviors, device information, referring URLs, session information, user
5 identifiers, and/or geolocation data. In other words, even when consumers like Plaintiffs tried to
6 protect their privacy by opting out of or rejecting cookies, Defendant failed to prevent cookies
7 from being transmitted to Third Parties, enabling them to track user behavior and
8 communications.

9 66. Some aspects of the operations of the Third Party cookies on the Website can be
10 observed using specialized tools that log incoming and outgoing Website network transmissions.
11 The following screenshot, obtained using one such tool, shows examples of Third-Party cookies
12 being transmitted from a Website user's device and browser to Third Parties even after the user
13 clicked the "Opt Out" button on the Website's popup cookie consent banner.

The screenshot displays the Hilton website's search interface for hotels in San Francisco, CA. The page shows search filters, suggested amenities like free breakfast and parking, and a list of hotels. The Hampton Inn San Francisco Downtown/Convention Center is highlighted with a 3.5 out of 5.0 rating. On the right, the Chrome Developer Tools Network tab is open, showing a list of HTTP requests to various domains including smetric.hilton.com, googleads.g.doubleclick.net, www.google.com, bat.bing.com, app.link, tr.snapchat.com, and maps.googleapis.com.

Name	Status	Domain
s27826185156894?AQ=1&ndh=...	200	smetric.hilton.com
s221030919132	200	smetric.hilton.com
?value=0&guid=ON&script=0&dat...	302	googleads.g.doubleclick.net
?value=0&guid=ON&script=0&dat...	302	googleads.g.doubleclick.net
dest5.html?d_nsid=0	200	hilton.demdex.net
?value=0&guid=ON&script=0&dat...	302	www.google.com
?value=0&guid=ON&script=0&dat...	302	www.google.com
0?ti=5116034&Ver=2&mid=b68fc...	204	bat.bing.com
_r?sdk=web2.80.0&t=12175237...	200	app.link
p	200	tr.snapchat.com
p	200	tr.snapchat.com
_r?sdk=web2.80.0&t=12175237...	200	app.link
_r?sdk=web2.80.0&t=12175237...	200	app.link
_r?sdk=web2.80.0&t=12175237...	200	app.link
wpt.json	204	cdn0.forter.com
?value=0&guid=ON&script=0&dat...	200	www.google.com.au
?value=0&guid=ON&script=0&dat...	200	www.google.com.au
proximanova-bold-webfont.woff	200	litmus.com
proximanova-regular-webfont.woff	200	litmus.com
controls.js	200	maps.googleapis.com
data:image/gif;base...	200	
recaptcha_en.js	200	www.gstatic.com
QuotaService.RecordEvent?1shtt...	200	maps.googleapis.com
bannermg?action=returns&dom...	200	consent.trustarc.com
pageview	200	api2.branch.io
noticemsg?action=returns&domai...	200	consent.trustarc.com
wpt.json	200	cdn0.forter.com
profile	200	api.hilton.io
api.js?onload=onloadCallback&re...	200	www.google.com
events	200	cdn3.forter.com
RC82eaa627218b4662b31d6046...	200	assets.adobedtm.com
log?domain=hiltongdpr.com&cou...	200	consent.trustarc.com
v1.7-519	200	consent.trustarc.com
vt?pb=1m51m41i1012i162i397...	200	maps.googleapis.com

67. The screenshot above shows the “Network” tab of Chrome Developer Tools, which contains a list of HTTP network traffic transmissions between the user’s browser and various third party websites while the user visited and interacted with Defendant’s Website at <https://www.hilton.com>. The screenshot depicts only network traffic occurring *after* the user opted out of cookies using the cookie banner. As shown above, despite the user’s rejection of all cookies by opting out, the user’s interactions with the Website resulted in the user’s browser making a large number of GET and POST HTTP requests to third party web domains like www.google.com; doubleclick.net; bing.com; tr.snapchat.com; etc., and others. As further shown in the right-hand column of the screenshot, the user’s browser sent cookies along with those HTTP requests to the third parties.

1 68. This screenshot demonstrates that the Website caused third-party cookie data and
2 users' Private Communications to be transmitted to Third Parties, even after consumers opted
3 out of or rejected all cookies and tracking technologies by clicking or selecting the "Opt Out"
4 button. All of these network calls are made to the Third Parties without the user's knowledge,
5 and despite the user's rejection of all cookies.

6 69. Website users' Private Communications, including their browsing history, visit
7 history, website interactions, user input data, demographic information, interests and
8 preferences, shopping behaviors, device information, referring URLs, session information, user
9 identifiers, and/or geolocation data, are surreptitiously obtained by the Third Parties via these
10 cookies.

11 70. As users interact with the Website, even after clicking or selecting the "Opt Out"
12 button, thereby opting out or rejecting the use of cookies and similar technologies for
13 personalized content, advertising, and analytics, as well as the sale or sharing of the user's
14 personal information with third parties for such functions, or other purposes, more data regarding
15 users' behavior and communications are sent to third parties, alongside the cookie data. The
16 third-party cookies that Defendant wrongfully allows to be stored on users' devices and
17 browsers, and to be transmitted to the Third Parties, enable the Third Parties to track and collect
18 data on users' behaviors and communications, including Private Communications, on the
19 Website. Because third-party cookies enable Third Parties to track users' behavior across the
20 Internet and across time, user data can be correlated and combined with other data sets to compile
21 comprehensive user profiles that reflect consumers' behavior, preferences, and demographics
22 (including psychological trends, predispositions, attitudes, intelligence, abilities, and aptitudes).
23 These Third Parties monetize user profiles for advertising, sales, and marketing purposes to
24 generate revenue and target advertising to Internet users. Advertisers can gain deep
25 understanding of users' behavioral traits and characteristics and target those users with
26 advertisements tailored to their consumer profiles and audience segments.

71. The Third Party code that the Website causes to be loaded and executed by the user's browser becomes a wiretap when it is executed because it enables the Third Parties—separate and distinct entities from the parties to the conversations—to use cookies to eavesdrop upon, record, extract data from, and analyze conversations to which they are not parties. When the Third Parties use their respective wiretaps on Website users' Private Communications, the wiretaps are not like tape recorders or “tools” used by one party to record the other. The Third Parties each have the capability to use the contents of conversations they collect through their respective wiretaps for their own purposes as described in more detail below.

E. Defendant's Conduct Violated Its Own Privacy Statement.

72. Defendant's aiding, agreeing with, employing, permitting, or otherwise enabling the Third Parties to track users' Private Communications on the Website using third-party cookies—even after those users click or select the “Opt Out” button—is particularly egregious given Defendant's additional written assurances in its Privacy Statement that users can, in fact, opt out of cookies and tracking technologies used on the Website. Specifically, Defendant represented to Plaintiffs and its users the following in the Privacy Statement:

If you would like to opt out of the sale of your personal information, you may do so by clicking on the banner that appears on any Hilton website when you access that site from an IP address that relates to California or by visiting our website at datarights.hilton.com or click the “Personal Data Requests” link at the bottom of any Hilton website to submit your request. Please note that when you opt out of cookies, tags, and pixels, that opt out only pertains to the device and the browser that you are using when you opt out. If you wish to opt out for other devices or browsers, you must opt out again when you are using those devices or browsers.

Privacy Statement (emphasis added.).

F. The Private Communications Collected As a Result of Third Party Cookies Transmitted When Visiting Defendant's Website.

1. Google Cookies

73. Defendant causes third party cookies to be transmitted to and from Website users' browsers and devices, even after users opt out of all cookies (including advertising and analytics

cookies) to and from the www.google.com and doubleclick.net domains. These domains are associated with Google LLC's digital advertising and analytics platform that collects user information via cookies to assist Google in performing data collection, behavioral analysis, user retargeting, and analytics.² Google serves targeted ads to web users across Google's ad network, which spans millions of websites and apps. Nearly 20% of web traffic is tracked by Google's DoubleClick cookies.³ Google's cookies help it track whether users complete specific actions after interacting with an ad (e.g., clicking a link or making a purchase) and provide analytic metrics that advertisers use to measure ad campaign performance. Further, by identifying users who have shown interest in certain products or content, Google's cookies enable its advertising platform to enable advertisers to show relevant ads to those users when they visit other websites within Google's ad network.⁴

74. Specifically, Google sends cookies when a web user visits a webpage that shows Google Marketing Platform advertising products and/or Google Ad Manager ads.⁵ "Pages with Google Marketing Platform advertising products or Google Ad Manager ads include ad tags that instruct browsers to request ad content from [Google's] servers. When the server delivers the ad content, it also sends a cookie. But a page doesn't have to show Google Marketing Platform advertising products or Google Ad Manager ads for this to happen; it just needs to include Google Marketing Platform advertising products or Google Ad Manager ad tags, which might load a click tracker or impression pixel instead." *Id.* As Google explains, "Google Marketing Platform advertising products and Google Ad Manager send a cookie to the browser after any impression, click, or other activity that results in a call to our servers." *Id.*

² See Our advertising and measurement cookies (available at <https://business.safety.google/adscookies/>).

³ See, e.g. <https://www.ghostery.com/whotracksme/trackers/doubleclick>.

⁴ See, e.g. About cross-channel remarketing in Search Ads 360 (available at <https://support.google.com/searchads/answer/7189623?hl=en>); About dynamic remarketing for retail (available at <https://support.google.com/google-ads/answer/6099158?hl=en&sjid=1196213575075458908-NC>).

⁵ See How Google Marketing Platform advertising products and Google Ad Manager use cookies (available at <https://support.google.com/searchads/answer/2839090?hl=en&sjid=1196213575075458908-NC>); see also Cookies and user identification (available at <https://developers.google.com/tag-platform/security/concepts/cookies>).

75. Google also uses cookies in performing analytical functions. As Google explains, “Google Analytics is a platform that collects data from [] websites and apps to create reports that provide insights into [] business[es].”⁶ “To measure a website ... [one] add[s] a small piece of JavaScript measurement code to each page on [a] site.” *Id.* Then, “[e]very time a user visits a webpage, the tracking code will collect ... information about how that user interacted with the page.” *Id.* Google Analytics enables website owners to “measure when someone loads a page, clicks a link, [] makes a purchase;” “completes a purchase;” “searches [] website or app;” “select content on [] website or app;” “views an item;” and “views their shopping cart.”⁷

76. Google’s cookies allow it to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information, (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data.⁸

77. For example, the Google software code that Defendant causes to be stored on and executed by the Website user’s device causes the following cookie data to be sent to Google’s domain, at <https://googleads.g.doubleclick.net>:

⁶ How Google Analytics Works (available at <https://support.google.com/analytics/answer/12159447?hl=en>).

⁷ Set up events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and Recommended events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>).

⁸ See About the Google Tag (available at <https://support.google.com/searchads/answer/7550511?hl=en>); How Floodlight Recognizes Users (available at <https://support.google.com/searchads/answer/2903014?hl=en>); How Google Ads tracks website conversions (available at <https://support.google.com/google-ads/answer/7521212>); Google Ads Help, Cookie: Definition (available at <https://support.google.com/google-ads/answer/2407785?hl=en>); About demographic targeting in Google Ads (available at https://support.google.com/searchads/answer/7298581?hl=en&sjid=1196213575075458908-NC&visit_id=638670675669576522-2267083756&ref_topic=7302618&rd=1); How Google Analytics Works (<https://support.google.com/analytics/answer/12159447>); Set up events (available at <https://developers.google.com/analytics/devguides/collection/ga4/events>); and Recommended events (available at <https://support.google.com/analytics/answer/9267735>).

Request	Header	Query	Body	Cookies	Raw	Summary	+	
Key	Value							
ar_debug	1							
DSID	AC1gg-SY_ZxxJNnFMtHMay_ivtrfWdqql-G2W5rQYjzoe1-qdg4DfTDgQS32mSMFLvuFxi6uinoJHMrpYvTrjDqu8Nv7BM9y4XimpA_DqUhNAbadInL6bMxMNxmHnwCC0cbHZqX85hTjaXuZQbGbBYYJ-LFVZDQpluzguq3mSCNV17KOG2_xpvn9BIOvMOxTuJU_2c3CkOS3tlrWEHS3dVdkBQH8cx_Fs-c_XH0rz4SN8RI5uLleoduMCACL45RFL0JLg17B7ufDaipHm2FnzBtERdISiL7xTEngkOkcv76cC1wOWBA3Y							
IDE	AHWqTUNg9BBfY34TIZoF7edf5mD17J-mC307xvYZMCIN_Y3yMVeEeqTia5A0T-OjDIE							

78. Google uses the “DSID” cookie to “identify a signed-in user on non-Google sites.”⁹ The “IDE” cookie is used “to personalize the ads [users] see” and “to show Google ads on non-Google sites.”¹⁰

79. Further, along with all of this data, the Google software code that Defendant causes to be stored on and executed by the user’s device causes the user’s “user-agent” information to be sent to Google:

user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
------------	---

80. The “user-agent” corresponds to the device and browser that the user has used to access the Website. In this example, the user-agent value corresponds to Google’s Chrome browser version 121, running on the Catalina version of macOS.¹¹

81. Finally, the data sent to Google contains the user’s IP address.

82. Because Google’s cookies operate across multiple sites (i.e., cross-site tracking), the cookie enables Google to track users as they navigate from one site to another, and to comprehensively observe and evaluate user behavior online. Google’s advertising platform

⁹ See <https://policies.google.com/technologies/cookies?hl=en-US>

¹⁰ See *id.*

¹¹ There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at <https://explore.whatismybrowser.com/useragents/parse>.

1 aggregates user data to create consumer profiles containing detailed information about a
2 consumer's behavior, preferences, and demographics and audience segments based on shared
3 traits (such as females, Millennials, etc.), and to perform targeted advertising and marketing
4 analytics.

5 83. Thus, the Google cookies used on the Website enable Google to track users'
6 interactions with advertisements to help advertisers understand how users engage with ads across
7 different websites. Further, the user data collected through the cookie enables the delivery of
8 personalized ads based on user interests and behaviors. For instance, if a user frequently visits
9 travel-related websites, Google will show her more travel-related advertisements. Further, the
10 collected data is used to generate reports for advertisers, helping them assess the performance of
11 their ad campaigns and make data-driven decisions (such as renaming their products). Further,
12 Google's advertising platform enables advertisers to retarget marketing, which Google explains
13 allows advertisers to "show previous visitors ads based on products or services they viewed on
14 your website. With messages tailored to your audience, dynamic remarketing helps you build
15 leads and sales by bringing previous visitors back to your website to complete what they
16 started."¹²

17 84. Further, in its "Shared Data Under Measurement Controller-Controller Data
18 Protection Terms," Google states: "Google can access and analyze the Analytics data customers
19 share with us to better understand online behavior and trends, and improve our products and
20 services—for example, to improve Google search results, detect and remove invalid advertising
21 traffic in Google Ads, and test algorithms and build models that power services like Google
22 Analytics Intelligence that apply machine-learning to surface suggestions and insights for
23 customers based on their analytics data and like Google Ads that applies broad models to
24 improve ads personalization and relevance. These capabilities are critical to the value of the
25 products we deliver to customers today."¹³ Thus, Google can have the capability to use the data

26 _____
27 ¹² Dynamic remarketing for web setup guide (available at <https://support.google.com/google-ads/answer/6077124>).

28 ¹³ Shared Data Under Measurement Controller-Controller Data Protection Terms (available at
<https://support.google.com/analytics/answer/9024351>).

1 it collects for understanding online behavior and trends, machine learning, and improving its
2 own products and services.

3 85. Defendant's integration of Google tracking into the Website was intentional. To
4 implement it, Hilton had to create one or more Google Ad and Google Analytics accounts, and
5 then add tags to its Website that caused the tracking pixels to be installed on user's computers
6 when they visited the Website. As part of this, Hilton obtained a Google ID that specifically
7 associated tracked data with its Website. Google's instructions for implementing such code
8 include an admonition to test the pixels to ensure they are functioning properly. This includes
9 specific notice to make sure that the data collection complies with privacy laws such as GDPR
10 and California Privacy Protection Act. Hilton obtained tracked data back from Google via
11 Google Ads and Google Analytics reporting.

12 2. Adobe Cookies

13 86. Defendant also causes third party cookies to be transmitted to and from Website
14 users' browsers and devices, even after users elect to opt out of cookies, to and from the
15 demdex.net and omtrdc.net domains. These domains are associated with Adobe Inc.'s
16 Audience Manager, a data management platform, Adobe's Marketing Cloud, and Adobe's
17 Experience Cloud Identity Service, a service which provides a universal, persistent ID to identify
18 visitors across all Adobe products.

19 87. These cookies are used to assign a unique identifier to each site visitor, which
20 enables Adobe to consistently recognize and track users across different sessions and domains
21 (i.e., cross-site tracking) and collect and synchronize user data to comprehensively observe and
22 evaluate user behavior online.¹⁴ These cookies enable Adobe to obtain and store at least the
23
24
25

26 ¹⁴ See, e.g., Adobe Experience League: Adobe Analytics cookies (available at
27 <https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics>); see also
28 Adobe Experience League: Audience Manager cookies (available at
<https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/audience-manager>).

following user data: (i) user identifier; (ii) website interactions; (iii) browsing history; (iv) visit history; (v) interests and preferences; and (vi) session information.¹⁵

88. Adobe aggregates this cookie data with other data from multiple channels and devices, including web analytics, CRM systems, and e-commerce platforms, to create consumer profiles containing detailed information about a consumer's behavior, preferences, and demographics, create audience segments based on shared traits (such as millennials, tech enthusiasts, etc.), and to enable targeted advertising and marketing analytics.¹⁶

89. Defendant has configured a subdomain it owns and operates, at smetric.hilton.com, to point directly to Adobe's endpoint, at hilton.com.ssl.sc.omtrdc.net.¹⁷

SuperTool Beta7

smetric.hilton.com **DNS Lookup**

a:smetric.hilton.com **Find Problems**

Type	Domain Name	Canonical Name	TTL
CNAME	smetric.hilton.com	hilton.com.ssl.sc.omtrdc.net	5 min

	Test	Result
✓	DNS Record Published	DNS Record found

¹⁵ See, e.g., Adobe Audience Manager User Guide: Data Collection Components (available at <https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/system-components/components-data-collection>).

¹⁶ See, e.g., Adobe Audience Manager User Guide: Understanding Calls to the Demdex Domain (available at <https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/reference/demdex-calls>); Adobe Experience Cloud Identity Service overview (available at <https://experienceleague.adobe.com/en/docs/id-service/using/intro/overview>); Adobe Audience Manager Features (available at <https://business.adobe.com/products/audience-manager/features.html>); see also Audience Manager Overview (available at <https://experienceleague.adobe.com/en/docs/audience-manager/user-guide/overview/aam-overview>).

¹⁷ Data obtained from <https://mxtoolbox.com> and <https://www.nslookup.io/>

DNS records for **smetric.hilton.com**

Cloudflare

Google DNS

Authoritative

Control D ▾

CNAME record

Canonical name

hilton.com.ssl.sc.omtrdc.net

90. The omtrdc.net domain is owned and operated by Adobe, and functions as a tracking server for Adobe Analytics.¹⁸

91. For example, when a user searches for hotels in San Francisco, the website causes the following type of data to be sent to Adobe Analytics at hilton.com.ssl.sc.omtrdc.net, via the smetric.hilton.com subdomain:

Request		Header	Query	Body	Cookies	Raw	Summary	+	⊟
Key		Value							
AQB		1							
ndh		1							
pf		1							
callback		s_c_il[1].doPostbacks							
et		1							
t		7%2F9%2F2023%2013%3A38%3A46%206%20420							
d.									
nsid		0							
jsonv		1							
.d									
mid		41702232992936575562205778250591185886							
aamlh		9							
ce		UTF-8							
pageName		Browser%3AEN%3AMultibrand%3ACategoryPage%3ALocations%3AUS%7CCA%3ASan%20Francisco							

¹⁸ See <https://experienceleague.adobe.com/en/docs/target/using/integrate/a4t/analytics-tracking-server>

g	https%3A%2F%2Fwww.hilton.com%2Fen%2Flocations%2Fusa%2Fcalifornia%2Fsan-francisco%2F%3FdatelessMvtChoice%3Db
cc	USD
events	event119
v27	Browser%3AEN%3AMultibrand%3ACategoryPage%3ALocations%3AUS%7CCA%3ASan%20Francisco
v59	multibrand
pe	lnk_o
pev2	AWS%20Chat%20-%20Chat%20Presented
s	2240x1260
c	30
j	1.6
v	N
k	Y
bw	649
bh	987
mcorgid	F0C120B3534685700A490D45%40Adobe Org
lrt	315
AQE	1

92. The “mid” parameter is Adobe’s unique user identifier that persists across sessions, used to identify a visitor in the Adobe ecosystem.¹⁹

93. The “pageName” and “g” parameters correspond to the name of the page and url that the user is browsing. In this case, the values of the parameters contain the user’s search string (“San Francisco”), revealing to Adobe that the user was searching for hotels in San Francisco.

94. Along with this data, the Adobe software code that Defendant causes to be stored on and executed by the user’s device causes the following cookies to be sent to Adobe:

¹⁹ See <https://experienceleague.adobe.com/en/docs/analytics/components/metrics/unique-visitors>

Request	Header	Query	Body	Cookies	Raw	Summary	+
Key	Value						
__lt_cid.47135154	86f46223-bb9d-4fd5-9e17-20f4b07c5533						
__lt_sid.47135154	0b20ae9e-910e4a98						
_abck	55FE5653E1A96C4359D0AC4CE3BAACE8~0~YAAQI/ TVFw1klvWKAQAAAXfbCwo8JYBslulZflsJAHUL7H+6noU4skl2A/ 7+R2g0Ps5y3DEgOzbZkGMZMeFWg6tiGO1qetwbYDdnXV/b/ qj1Y4JXOKRpTJLAxqkE2lGIR1VcmYoJArzy/ UgiYLVl8ojQqaBAJYmR+V+v6qJmxMzMwqm8gMMMOBAG5wwCCt7R3Lk5O XxTmQHoAUifKCVMWiMDhvmGl7gpGQciSyr6TAi9fGfbxr+xOUj18X5lkyi8KE/ 9BknZ4g0b// GBuvGZL4C4veXWLusW2VjZFFlj+nkV+mxUdgKzKjyer3Eg0glRjyc5LqrkbKT prSnOcm+l60+bx9ijn8qtGGcLRHwG3ywGTOMdTv+F1Sp3mQSF4ib9kBaNnc QnTm0VF2fEozYKdgdZC8uNmYOK3hUCjX8IXmE9at4Rc0HiBhzCGmljkPDe0 32wp+Gm9J/~1~1~1696714567						
_fbp	fb.1.1696711017940.1438213681						
_gcl_au	1.1.1648324264.1696711019						
_pin_unauth	dWlKPVptWmxaakkzWmpFdE1tUmpZeTawT1dGaExUazBZV0l0WldFek5tWXI PV1ZsWmpkag						
_scid	5b9e5461-f48f-45c6-836e-1a10256b2b4f						
_scid_r	5b9e5461-f48f-45c6-836e-1a10256b2b4f						
_sctr	1%7C1696662000000						
_uetSid	42436670655111ee86b3339bdb3d083b						
_uetvid	42436300655111ee9aaf836fc1ac976a						
aam_uuid	41678662076505314832203624045623958161						
ak_bmsc	EC63D9FE7F41756E8D1A3D8A9F647B39~0000000000000000000000 000000~YAAQI/TVF/ hJLvWKAQAAonbbCxXugb33S9EyRd13hpflYwaTb5KKA0pGQmqaoWkT/ mOmleEhMdVBNdSyAmzUoPEirjvv3N+f0dCzd0u5F+OGLBkSaRKvVx4ADP aE2NkCWK18j/NQnOtpj/SE8nbqA6/ACPMK9/ nGSOWnv6losrkH+398eD7vgxeq5CXSEmpdjybv5q5lRvkJhWKlbeu9pyBklK WK1WAj0zbb0qaTqAL8C7bT+B48BRQs7YvPaU6JZMg2tXfVYSNoF+6jCoW8 Mpt8y5OJqueHSHQKIRODqpcXfg7/ g4pBMaSRoBUDKZeimoxvrNpIYSKcaOEcaTYXoxFN0P6vsDqnOOcZTUx5Kd a+nXgspgtA3FfwMktPY6eyuJrhlg5PkSikQ==						
AKA_A2	A						
AMCV_F0C120B3534685700A 490D45%40AdobeOrg	179643557%7CMCIDTS%7C19638%7CMCMID%7C41702232992936575 562205778250591185886%7CMCAAMLH-1697315816%7C9%7CMCAA MB-1697315816%7CRKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ 3xzPWQmdj0y%7CMCOPTOUT-1696718216s%7CONE%7CMCAID%7CN ONE%7CvVersion%7C5.5.0						
AMCVS_F0C120B3534685700 A490D45%40AdobeOrg	1						
bm_sv	D0BFA4AAE349223367052DC00ADEF1C0~YAAQm/ TVF4Q0pgCLAQAASZdCxX1jEdwkg4Yu5wUpEC7cy+5TCw+zWxkb1Eod9 MPSvUgyoNeZvQZnqRJXuLA3NxoicM6j8KXSEbdYL97B43lt0r77emqS9LWz W5qRD1n5Wextf2UmfJgrfx/ WgnJQug8OQAGh2yNtlq8SBPJX7Vfo9Mmbqo3rguc1lfUq72tE/ dNawtnWdGKiv/ bAKOVpZ6REL5T46SPuLprFwrgsj56YPOU0xbjKSeQBi3oLut8~1						
bm_sz	CC4D379CE9706CEA61F79A2F876F9AFE~YAAQI/ TVF8ZiLWKAQAANDbCxXsZm8bKlyoWju9dcHTLEsOJMHv3+LsJfShzVUM lxwzYZGfz4MGtHKDL6cWQOn+feXvmWuYAyVDUOR4L69QU0kenEdUng6o6t 3Mxomc43CepsfLAJ7xhRWW3z+zOgbl6+T5FdBEy/emrbQPpgpx/r/ fyge+IW0G1iINU+LcN1E8wBbdWUTlJLuMYPO4Dm3U9iibCifQBgrlEpLNBxf ZrAdTF+Li6+coew5dVklMhZbUQxB3CaSIITMRq6zK+N1FFU6XkX41OkNbu KGmBJOYmeg=~4403777~3687223						
cmapi_cookie_privacy	permit 1 required						
cmapi_gtm_bl	ga-ms-ua-ta-asp-bzi-sp-awct-cts-csm-img-flc-fls-mpm-mpr-m6d-tc-tdc						
dtCookie	v_4_srv_3_sn_LB7U36ABIP71KV2HH5AITGDS0E4A2LFG_app-3A0da30f11 c94bda74_1_ol_0_perc_100000_mul_1_rcs-3Acss_0						
dtPC	3\$511123880_920h16vQQLWTRTRLPPOMGUUAHFPTAFHUFMKHCv-0e0						
dtSa	-						
fltk	segID%3D15195757						

forterToken	5f65946e5744421c9e4d5f4226592a0f_1696711124332__UDF43-m4_15ck
ftr_blst_1h	1696711016504
gpv_v9	Browser%3AEN%3AMultibrand%3ACategoryPage%3ALocations%3AUS%7CCA%3ASan%20Francisco
notice_behavior	implied,us
notice_gdpr_prefs	0:
notice_preferences	0:
RT	"z=1&dm=hilton.com&si=a35c06aa-f5b9-4725-9ffe-2d615a847068&ss=lnghxfgy&sl=2&se=p0&tt=7tk&bcn=%2F%2F17de4c15.akstat.io%2F"
rxVisitor	16967110125660MT443UVP6CVUFVIJ7O9PDDOAKHPM22U
rxvt	1696712926006 1696711012567
s_cc	true
s_ecid	MCMID%7C41702232992936575562205778250591185886
s_sq	%5B%5BB%5D%5D
TAsessionID	c4e474ef-81c3-4e5b-8413-fb50ed31bbae NEW
TMS	web%3D17836315%2Cweb-app%3D15195757%2Cweb-app%3D16416847%2CWeb-app%3D17146407%2Cweb-app%3D17347117%2Cweb-app%3D17567317%2Cweb-app%3D17727890%2Cweb-app%3D19484989%2Cweb-app%3D21881915

95. According to Adobe documentation, the cookies beginning with “AMCV_...” and “AMCVS_...” are tracking cookies, enabling Adobe to identify the unique user and to track them across other Adobe-integrated websites.²⁰

96. The “s_ecid” cookie is used to store the Experience Cloud ID (ECID) or MID, further enabling Adobe to track the user.²¹

97. In addition, because of the way Defendant has configured its smetric.hilton.com subdomain, a large number of non-Adobe cookies are sent to Adobe, including cookies typically used by Microsoft Ads, Google Ads, Facebook, Pinterest, and Snap. For example, the “_fbp” cookie above is a Facebook cookie, and can be used to identify the user’s Facebook account.

98. Further, along with all of this data, the Adobe software code that Defendant causes to be stored on and executed by the user’s device causes the user’s “user-agent” information to be sent to Adobe:

²⁰ See <https://experienceleague.adobe.com/en/docs/id-service/using/intro/cookies>

²¹ See <https://experienceleague.adobe.com/en/docs/core-services/interface/data-collection/cookies/analytics>

Key	Value
user-agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36

As discussed above with respect to Google, the “user-agent” corresponds to the device and browser that the user has used to access the Website. In this example, the user-agent value corresponds to Google’s Chrome browser version 121, running on the Catalina version of macOS.²²

99. Finally, the data sent to Adobe includes the user’s IP address.

100. Defendant’s integration of Adobe tracking into the Website was intentional. To implement it, Hilton had to create one or more Adobe Experience Platform (formerly, Adobe Launch) accounts, and then add Adobe tags to its Website that caused the Adobe tracking pixels to be installed on user’s computers when they visited the Website. As part of this, Hilton obtained an Adobe registration that specifically associated tracked data with its Website. Adobe’s instructions for implementing such code include an admonition to test the pixels to ensure they are functioning properly. This includes specific notice to make sure that the data collection complies with privacy laws such as GDPR and the CCPA. Hilton obtained tracked data back from Adobe via Adobe Analytics/Reporting.

3. Additional Cookies

101. Defendant also causes third party cookies to be transmitted to and from Website users’ browsers and devices, even after users elect to opt out of all cookies, to and from other domains, including bat.bing.com and tr.snapchat.com.

102. The bat.bing.com domain is associated with associated with Bing, Microsoft’s search engine, as well as Microsoft’s digital advertising and analytics platforms. When a webpage loads a bat.bing.com cookie, it “tells Microsoft Advertising about the user visits to [the]

²² There are many tools on the web that are capable of parsing user-agent strings to determine what browser and operating system they pertain to. One such tool is located at <https://explore.whatismybrowser.com/useragents/parse>.

webpage.”²³ Microsoft uses bat.bing.com cookies to “record[] what customers do on [a] website and send[] that information to Microsoft Advertising.”²⁴

103. Bat.bing.com cookies collect consumers’ (i) search history and browsing history, (ii) visit history, (iii) website interactions, (iv) user input data, (v) demographic information (including zip code²⁵; gender²⁶; age²⁷ (including identifying whether that person is a minor or not)); (vi) interests and preferences, (vii) shopping behaviors, (viii) device information, (ix) referring URLs, (x) session information, (xi) user identifiers, and (xii) geolocation data (including IP addresses). Microsoft updates this information each time a user clicks on a website hosting a third-party bat.bing.com cookie.

104. Bat.bing.com cookies help Microsoft track users’ interactions with ads (e.g., clicking a link or making a purchase) and provide valuable metrics that advertisers use to measure ad campaign performance. Further, bat.bing.com cookies allow Microsoft to obtain and store at user data to “help [website owners] focus a campaign or ad group on potential audiences who meet [website owners’] specific criteria, so [website owners] can increase the chance that [consumers] see [website owners’] ads.”²⁸ Further, bat.bing.com cookies offer valuable “conversion tracking,” which is a “measure [of] the ROI (return on investment) of your advertising campaign by letting [website owners] assign a monetary value to the activities people complete on [their] website after clicking [website owners’] ad.”²⁹

²³ Microsoft Advertising Help: Everything you need to know about setting up UET (available at <https://help.ads.microsoft.com/apex/index/3/en/56959#:~:text=The%20most%20important%20request%20is,making%20when%20your%20webpage%20loads>).

²⁴ Microsoft Advertising Help: What is UET and how can it help me? (available at <https://help.ads.microsoft.com/#apex/ads/en/56960/1>).

²⁵ Microsoft Advertising Help: Legal, privacy, and personalization (available at <https://help.ads.microsoft.com/#apex/ads/en/60212/0>).

²⁶ *Id.*

²⁷ *Id.*

²⁸ *Id.*

²⁹ Microsoft Advertising Help: What is conversion tracking? (available at <https://help.ads.microsoft.com/#apex/ads/en/56680/2>).

105. Microsoft also utilizes bat.bing.com data for its own purposes, including by using the data to tailor content and target advertisements to users. This profile enables Microsoft to deliver highly targeted ads within Microsoft's extensive advertising network. Microsoft's revenue from its advertising network program has exceeded \$10 billion as of 2022.³⁰

106. The subdomain tr.snapchat.com is associated with Snap Inc. (SnapChat), a social media company that uses its cookies to measure users' conduct across distinct websites to help advertisers target ads.³¹ SnapChat uses tr.snapchat.com to collect data on browsing history, choices, and interactions with advertisements.³² This data helps Snapchat personalize ad content and track users across the internet.³³

107. These cookies allow these Third Parties to obtain and store at least the following user data: (i) browsing history, (ii) visit history, (iii) website interactions, (iv) demographic information, (v) interests and preferences, (vi) shopping behaviors, (vii) device information, (viii) referring URLs, (ix) session information, (x) user identifiers, and/or (xi) geolocation data.

108. Defendant's integration of Snapchat Snap Pixel tracking into the Website was intentional. To implement it, Hilton had to create one or more Snapchat Ads Manager accounts, and then add Snapchat tags to its Website that caused the Snapchat tracking pixels to be installed on users' computers when they visited the Website. As part of this, Hilton obtained a Snapchat registration that specifically associated tracked data with its Website. Snapchat's instructions for implementing such code include an admonition to test the pixels to ensure they are functioning properly. This includes specific notice to make sure that the data collection complies with privacy laws. Hilton obtained tracked data back from Snapchat via Snapchat Ads Manager reporting.

³⁰ Microsoft's ad revenue hit \$10B, and it's investing — is it a sleeping giant about to wake? (Ronan Shields) January 27, 2022 (available at <https://digiday.com/media/microsofts-ad-revenue-hit-10b-and-its-investing-is-a-sleeping-giant-about-to-wake/>).

³¹ See <https://snapdiscoveries.com/what-is-tr-snapchat-com-is-used-for>.

³² *Id.*

³³ *Id.*

G. The Private Communications Collected are Valuable.

109. The Personal Communications that the Third Parties track and collect by way of the cookies on the Website are valuable to Defendant as well as the Third Parties. Defendant can use the data to create and analyze the performance of marketing campaigns, website design, product placement, and target specific users or groups of users for advertisements. For instance, if Defendant wanted to market certain of its hotel and resorts to consumers, Defendant could use the data collected by the Third Parties to monitor users who visit webpages related to specific products, then advertise similar products to those particular users when they visit other webpages. The third-party cookies also enable Defendant to target online advertisements to users when they visit *other* websites, even those completely unrelated to Defendant and its products.

110. Data about users' browsing history enables Defendant to spot patterns in users' behavior on the Website and their interests in, among other things, Defendant's hotel and resorts. On a broader scale, it enables Defendant to gain an understanding of trends happening across its brands and across the hospitality market. All of this helps Defendant further monetize its Website and maximize revenue by collecting and analyzing user data.

111. The value of the Private Communications tracked and collected by the Third Parties using cookies on the Website can be quantified. Legal scholars observe that "[p]ersonal information is an important currency in the new millennium."³⁴ Indeed, "[t]he monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend." *Id.* "Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information." *Id.*

112. Numerous empirical studies quantify the appropriate value measure for personal data. Generally, the value of personal data is measured as either the consumer's willingness to accept compensation to sell her data or the consumer's willingness to pay to protect her information.

³⁴ See Paul M. Schwartz, *Property, Privacy and Personal Data*, 117 Harv. L. Rev. 2055, 2056–57 (2004).

1 113. Through its false representations and aiding, agreeing with, employing,
2 permitting, or otherwise enabling the Third Parties to track users' Private Communications on
3 the Website using third-party cookies, Defendant is unjustly enriching itself at the cost of
4 consumer privacy and choice, when the consumer could otherwise have the ability to choose if
5 and how they would monetize their data.

6 **PLAINTIFFS' EXPERIENCES**

7 **Plaintiff Shah**

8 114. In or around March 2023, Plaintiff Shah visited the Website to browse
9 information about Hilton's hotels and resorts.

10 115. When Plaintiff Shah visited the Website, the Website immediately presented him
11 with Defendant's popup cookie consent banner, which provided the option to select the "Opt
12 Out" button. Plaintiff Shah viewed Defendant's representation on the popup cookie consent
13 banner that, "We use cookies and similar technologies to provide you with personalized content,
14 improve site performance, and conduct analytics. We also work with third parties to show you
15 content and advertisements for products and services you might like. These third parties use
16 cookies on this site to process your personal data for their own purposes. If you wish to opt out
17 of cookies and similar technologies, please click the Opt Out button." Plaintiff Shah also viewed
18 Defendant's additional representation that users could "Opt Out" of cookies by clicking the
19 button.

20 116. Consistent with his typical practice in rejecting or otherwise opting out of the
21 placement or use of cookies and tracking technologies, Plaintiff Shah selected and clicked the
22 "Opt Out" button. Plaintiff Shah believed that selecting the "Opt Out" button on the popup
23 cookie consent banner found on the Website would allow him to opt out of, decline, and/or reject
24 all cookies and other tracking technologies (inclusive of those cookies that cause the disclosure
25 of user data to third-parties for the purposes of providing personalized content, advertising, and
26 analytics services).

27 117. In selecting the "Opt Out" button, Plaintiff Shah gave Defendant notice that he
28 did not consent to the use or placement of cookies and tracking technologies while browsing the

1 Website. Further, Plaintiff Shah specifically opted out of or rejected, based on Defendant's
2 representations, those cookies used to "personalize[] content, improve site performance, and
3 conduct analytics ... [and] advertisements" and share users' "personal data" with third parties.
4 In reliance on these representations and promises, only then did Plaintiff Shah continue browsing
5 the Website.

6 118. Even before the popup cookie consent banner appeared on the screen, Defendant
7 nonetheless caused cookies and tracking technologies, including those used for personalized
8 content, advertising, and analytics, to be placed on Plaintiff Shah's device and/or transmitted to
9 the Third Parties along with user data, without Plaintiff Shah's knowledge. Accordingly, the
10 popup cookie consent banner's representation to Plaintiff Shah that he could opt out of or reject
11 the use and/or placement of cookies and tracking technologies while he browsed the Website
12 was false. Contrary to what Defendant made Plaintiff Shah believe, he did not have a choice
13 about whether third-party cookies would be placed on his device and/or transmitted to the Third
14 Parties along with his user data; rather, Defendant had already caused that to happen.

15 119. Plaintiff Shah browsed the Website, seeking hotel rooms that were available for
16 him. Plaintiff Shah engaged in Private Communications by typing in search strings for the
17 location(s) he wished to visit (e.g., "Puerto Vallarta"), and input various options (e.g., dates of
18 visit, number of visitors). He selected filters to prioritize display of types of rooms he favored.
19 He also selected some of the displayed properties and clicked through to look at them in more
20 detail. As each property and room was clicked, URLs containing Private Communications in
21 the form of details input by Plaintiff Shah (e.g., the location, room type, number of visitors, dates
22 of visit, etc.) were transmitted to Hilton and captured by Third Party cookies and recorded.

23 120. Then, as Plaintiff Shah continued to browse the Website in reliance on the
24 promises Defendant made in the cookie consent banner, and despite Plaintiff Shah's clear
25 rejection of the use and/or placement of such cookies and tracking technologies, Defendant
26 nonetheless continued to cause the placement and/or transmission of cookies along with user
27 data, including those involved in providing personalized content, advertising, and analytics from
28

1 the Third Parties on his device. In doing so, Defendant permitted the Third Parties to track and
2 collect Plaintiff Shah's Private Communications as Plaintiff Shah browsed the Website. On
3 information and belief, such tracking collected personal information of Plaintiff Shah, including
4 browsing history, visit history, website interactions, user input data and search parameters
5 (including search strings corresponding to Plaintiffs' dates and location of travel, number of
6 companions, and lodging preferences), demographic information, interests and preferences,
7 shopping behaviors, device information, referring URLs, session information, user identifiers,
8 and/or geolocation data.

9 121. Defendant's representations that consumers could "Opt Out" of cookies while
10 Plaintiff Shah and users browsed the Website, or at least those involved in providing
11 personalized content, advertising, and analytics services, were untrue. Had Plaintiff Shah known
12 this fact, he would not have used the Website. Moreover, Plaintiff Shah reviewed the popup
13 cookie consent banner and Privacy Statement prior to using the Website. Had Defendant
14 disclosed that it would continue to cause cookies and tracking technologies to be stored on
15 consumers' devices even after they choose to reject cookies, Plaintiff Shah would have noticed
16 it and would not have used the Website or, at a minimum, he would have interacted with the
17 Website differently.

18 122. Plaintiff Shah continues to desire to browse content featured on the Website.
19 Plaintiff Shah would like to browse websites that do not misrepresent that users can opt out of
20 or reject cookies and tracking technologies. If the Website were programmed to honor users'
21 requests to opt out of cookies and tracking technologies, Plaintiff Shah would likely browse the
22 Website again in the future, but will not do so until then. Plaintiff Shah regularly visits websites
23 that feature content similar to that of the Website. Because Plaintiff Shah does not know how the
24 Website is programmed, which can change over time, and because he does not have the technical
25 knowledge necessary to test whether the Website honors users' requests to opt out of cookies
26 and tracking technologies, Plaintiff Shah will be unable to rely on Defendant's representations
27 when browsing the Website in the future absent an injunction that prohibits Defendant from
28

1 making misrepresentations on the Website. The only way to determine what network traffic is
2 sent to third parties when visiting a website is to use a specialized tool such as Chrome Developer
3 Tools. As the name suggests, such tools are designed for use by “developers” (i.e., software
4 developers), whose specialized training enables them to analyze the data underlying the HTTP
5 traffic to determine what data, if any, is being sent to whom. Plaintiff Shah is not a software
6 developer and has not received training with respect to HTTP network calls.

7 **Plaintiff Gabrielli**

8 123. In or around August 2024 and November 2024, Plaintiff Gabrielli visited the
9 Website to browse information about Hilton’s hotels and resorts.

10 124. When Plaintiff Gabrielli visited the Website, the Website immediately presented
11 him with Defendant’s popup cookie consent banner, which provided the option to select the “Opt
12 Out” button. Plaintiff Gabrielli viewed Defendant’s representation on the popup cookie consent
13 banner that, “We use cookies and similar technologies to provide you with personalized content,
14 improve site performance, and conduct analytics. We also work with third parties to show you
15 content and advertisements for products and services you might like. These third parties use
16 cookies on this site to process your personal data for their own purposes. If you wish to opt out
17 of cookies and similar technologies, please click the Opt Out button.” Plaintiff Gabrielli also
18 viewed Defendant’s additional representation that users could “Opt Out” of cookies by clicking
19 the button.

20 125. Consistent with his typical practice in rejecting or otherwise opting out of the
21 placement or use of cookies and tracking technologies, Plaintiff Gabrielli selected and clicked
22 the “Opt Out” button. Plaintiff Gabrielli believed that selecting the “Opt Out” button on the
23 popup cookie consent banner found on the Website would allow him to opt out of, decline, and/or
24 reject all cookies and other tracking technologies (inclusive of those cookies that cause the
25 disclosure of user data to third-parties for the purposes of providing personalized content,
26 advertising, and analytics services).

1 126. In selecting the “Opt Out” button, Plaintiff Gabrielli gave Defendant notice that
2 he did not consent to the use or placement of cookies and tracking technologies while browsing
3 the Website. Further, Plaintiff Gabrielli specifically opted out of or rejected, based on
4 Defendant’s representations, those cookies used to “personalize[] content, improve site
5 performance, and conduct analytics ... [and] advertisements” and share users’ “personal data”
6 with third parties. In reliance on these representations and promises, only then did Plaintiff
7 Gabrielli continue browsing the Website.

8 127. Even before the popup cookie consent banner appeared on the screen, Defendant
9 nonetheless caused cookies and tracking technologies, including those used for personalized
10 content, advertising, and analytics, to be placed on Plaintiff Gabrielli’s device and/or transmitted
11 to the Third Parties along with user data, without Plaintiff Gabrielli’s knowledge. Accordingly,
12 the popup cookie consent banner’s representation to Plaintiff Gabrielli that he could opt out of
13 or reject the use and/or placement of cookies and tracking technologies while he browsed the
14 Website was false. Contrary to what Defendant made Plaintiff Gabrielli believe, he did not have
15 a choice about whether third-party cookies would be placed on his device and/or transmitted to
16 the Third Parties along with his user data; rather, Defendant had already caused that to happen.

17 128. Plaintiff Gabrielli browsed the Website, seeking hotel rooms that were available
18 for him. Plaintiff Gabrielli engaged in Private Communications by typing in search strings for
19 the location(s) he wished to visit (e.g., Irvine, California), and input various options (e.g., dates
20 of visit, number of visitors, distance from a specific location in Irvine). He selected filters to
21 prioritize display of types of rooms he favored (e.g., Price). He also selected some of the
22 displayed properties and clicked through to look at them in more detail. As each property and
23 room was clicked, URLs containing Private Communications in the form of details input by
24 Plaintiff Gabrielli (e.g., the location, room type, number of visitors, dates of visit, price, etc.)
25 were transmitted to Hilton and captured by Third Party cookies and recorded.

26 129. Then, as Plaintiff Gabrielli continued to browse the Website in reliance on the
27 promises Defendant made in the cookie consent banner, and despite Plaintiff Gabrielli’s clear
28

1 rejection of the use and/or placement of such cookies and tracking technologies, Defendant
2 nonetheless continued to cause the placement and/or transmission of cookies along with user
3 data, including those involved in providing personalized content, advertising, and analytics from
4 the Third Parties on his device. In doing so, Defendant permitted the Third Parties to track and
5 collect Plaintiff Gabrielli's Private Communications as Plaintiff Gabrielli browsed the Website.
6 On information and belief, such tracking collected personal information of Plaintiff Gabrielli,
7 including browsing history, visit history, website interactions, user input data and search
8 parameters (including search strings corresponding to Plaintiffs' dates and location of travel,
9 number of companions, and lodging preferences), demographic information, interests and
10 preferences, shopping behaviors, device information, referring URLs, session information, user
11 identifiers, and/or geolocation data.

12 130. Defendant's representations that consumers could "Opt Out" of cookies while
13 Plaintiff Gabrielli and users browsed the Website, or at least those involved in providing
14 personalized content, advertising, and analytics services, were untrue. Had Plaintiff Gabrielli
15 known this fact, he would not have used the Website. Moreover, Plaintiff Gabrielli reviewed the
16 popup cookie consent banner and Privacy Statement prior to using the Website. Had Defendant
17 disclosed that it would continue to cause cookies and tracking technologies to be stored on
18 consumers' devices even after they choose to reject cookies, Plaintiff Gabrielli would have
19 noticed it and would not have used the Website or, at a minimum, he would have interacted with
20 the Website differently.

21 131. Plaintiff Gabrielli continues to desire to browse content featured on the Website.
22 Plaintiff Gabrielli would like to browse websites that do not misrepresent that users can opt out
23 of or reject cookies and tracking technologies. If the Website were programmed to honor users'
24 requests to opt out of cookies and tracking technologies, Plaintiff Gabrielli would likely browse
25 the Website again in the future, but will not do so until then. Plaintiff Gabrielli regularly visits
26 websites that feature content similar to that of the Website. Because Plaintiff Gabrielli does not
27 know how the Website is programmed, which can change over time, and because he does not
28

1 have the technical knowledge necessary to test whether the Website honors users' requests to
2 opt out of cookies and tracking technologies, Plaintiff Gabrielli will be unable to rely on
3 Defendant's representations when browsing the Website in the future absent an injunction that
4 prohibits Defendant from making misrepresentations on the Website. The only way to determine
5 what network traffic is sent to third parties when visiting a website is to use a specialized tool
6 such as Chrome Developer Tools. As the name suggests, such tools are designed for use by
7 "developers" (i.e., software developers), whose specialized training enables them to analyze the
8 data underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff
9 Gabrielli is not a software developer and has not received training with respect to HTTP network
10 calls.

11 **Plaintiff Wiley**

12 132. In or around spring 2023 and July 2024, Plaintiff Wiley visited the Website to
13 browse information about Hilton's hotels and resorts.

14 133. When Plaintiff Wiley visited the Website, the Website immediately presented her
15 with Defendant's popup cookie consent banner, which provided the option to select the "Opt
16 Out" button. Plaintiff Wiley viewed Defendant's representation on the popup cookie consent
17 banner that, "We use cookies and similar technologies to provide you with personalized content,
18 improve site performance, and conduct analytics. We also work with third parties to show you
19 content and advertisements for products and services you might like. These third parties use
20 cookies on this site to process your personal data for their own purposes. If you wish to opt out
21 of cookies and similar technologies, please click the Opt Out button." Plaintiff Wiley also viewed
22 Defendant's additional representation that users could "Opt Out" of cookies by clicking the
23 button.

24 134. Consistent with her typical practice in rejecting or otherwise opting out of the
25 placement or use of cookies and tracking technologies, Plaintiff Wiley selected and clicked the
26 "Opt Out" button. Plaintiff Wiley believed that selecting the "Opt Out" button on the popup
27 cookie consent banner found on the Website would allow her to opt out of, decline, and/or reject
28

1 all cookies and other tracking technologies (inclusive of those cookies that cause the disclosure
2 of user data to third-parties for the purposes of providing personalized content, advertising, and
3 analytics services).

4 135. In selecting the “Opt Out” button, Plaintiff Wiley gave Defendant notice that she
5 did not consent to the use or placement of cookies and tracking technologies while browsing the
6 Website. Further, Plaintiff Wiley specifically opted out of or rejected, based on Defendant’s
7 representations, those cookies used to “personalize[] content, improve site performance, and
8 conduct analytics ... [and] advertisements” and share users’ “personal data” with third parties.
9 In reliance on these representations and promises, only then did Plaintiff Wiley continue
10 browsing the Website.

11 136. Even before the popup cookie consent banner appeared on the screen, Defendant
12 nonetheless caused cookies and tracking technologies, including those used for personalized
13 content, advertising, and analytics, to be placed on Plaintiff Wiley’s device and/or transmitted
14 to the Third Parties along with user data, without Plaintiff Wiley’s knowledge. Accordingly, the
15 popup cookie consent banner’s representation to Plaintiff Wiley that she could opt out of or reject
16 the use and/or placement of cookies and tracking technologies while she browsed the Website
17 was false. Contrary to what Defendant made Plaintiff Wiley believe, she did not have a choice
18 about whether third-party cookies would be placed on her device and/or transmitted to the Third
19 Parties along with her user data; rather, Defendant had already caused that to happen.

20 137. Plaintiff Wiley browsed the Website, seeking hotel rooms that were available for
21 her. Plaintiff Wiley engaged in Private Communications by typing in search strings for the
22 location(s) she wished to visit (e.g., Dallas, Texas), and input various options (e.g., dates of visit,
23 number of visitors). She selected filters such as price, rating, brand, guest services, dining, hotel
24 features, fitness & health, recreation, hotel type, and business & work (e.g., price, rooms with
25 kitchen, free breakfast). She also selected some of the displayed properties and clicked through
26 to look at them in more detail. As each property and room was clicked, URLs containing Private
27 Communications in the form of details input by Plaintiff Wiley (e.g., the location, room type,
28

1 number of visitors, dates of visit, etc.) were transmitted to Hilton and captured by Third Party
2 cookies and recorded.

3 138. Then, as Plaintiff Wiley continued to browse the Website in reliance on the
4 promises Defendant made in the cookie consent banner, and despite Plaintiff Wiley's clear
5 rejection of the use and/or placement of such cookies and tracking technologies, Defendant
6 nonetheless continued to cause the placement and/or transmission of cookies along with user
7 data, including those involved in providing personalized content, advertising, and analytics from
8 the Third Parties on her device. In doing so, Defendant permitted the Third Parties to track and
9 collect Plaintiff Wiley's Private Communications as Plaintiff Wiley browsed the Website. On
10 information and belief, such tracking collected personal information of Plaintiff Wiley, including
11 browsing history, visit history, website interactions, user input data and search parameters
12 (including search strings corresponding to Plaintiffs' dates and location of travel, number of
13 companions, and lodging preferences), demographic information, interests and preferences,
14 shopping behaviors, device information, referring URLs, session information, user identifiers,
15 and/or geolocation data.

16 139. Defendant's representations that consumers could "Opt Out" of cookies while
17 Plaintiff Wiley and users browsed the Website, or at least those involved in providing
18 personalized content, advertising, and analytics services, were untrue. Had Plaintiff Wiley
19 known this fact, she would not have used the Website. Moreover, Plaintiff Wiley reviewed the
20 popup cookie consent banner and Privacy Statement prior to using the Website. Had Defendant
21 disclosed that it would continue to cause cookies and tracking technologies to be stored on
22 consumers' devices even after they choose to reject cookies, Plaintiff Wiley would have noticed
23 it and would not have used the Website or, at a minimum, she would have interacted with the
24 Website differently.

25 140. Plaintiff Wiley continues to desire to browse content featured on the Website.
26 Plaintiff Wiley would like to browse websites that do not misrepresent that users can opt out of
27 or reject cookies and tracking technologies. If the Website were programmed to honor users'
28

1 requests to opt out of cookies and tracking technologies, Plaintiff Wiley would likely browse the
2 Website again in the future, but will not do so until then. Plaintiff Wiley regularly visits websites
3 that feature content similar to that of the Website. Because Plaintiff Wiley does not know how
4 the Website is programmed, which can change over time, and because she does not have the
5 technical knowledge necessary to test whether the Website honors users' requests to opt out of
6 cookies and tracking technologies, Plaintiff Wiley will be unable to rely on Defendant's
7 representations when browsing the Website in the future absent an injunction that prohibits
8 Defendant from making misrepresentations on the Website. The only way to determine what
9 network traffic is sent to third parties when visiting a website is to use a specialized tool such as
10 Chrome Developer Tools. As the name suggests, such tools are designed for use by "developers"
11 (i.e., software developers), whose specialized training enables them to analyze the data
12 underlying the HTTP traffic to determine what data, if any, is being sent to whom. Plaintiff Wiley
13 is not a software developer and has not received training with respect to HTTP network calls.

14 **HILTON'S KNOWLEDGE AND INTENT TO AID THIRD PARTIES**

15 141. As discussed herein, the decision to incorporate software code and settings that
16 caused and allowed Third Party cookies to be placed on visitors' browsing devices was Hilton's.
17 It acted intentionally to include that code in its Website, and thus knew that the code was being
18 called.

19 142. Hilton also created and implemented the cookie banner and privacy selection
20 windows for its Website, and thus knew how they behaved and intended them to work in that
21 manner. Thus, it had actual and/or constructive knowledge that its Website was calling the Third
22 Party cookies and causing them to be installed to enable tracking, even for those visitors who
23 had elected to "opt-out" of such tracking, and it intended them to work in that manner, as
24 demonstrated by its decision to allow them to continue to perform in that manner.

25 143. Through the actions above, Hilton gave substantial assistance to the Third Parties
26 in accomplishing a tortious and unlawful result. The Third Parties' actions are tortious because
27 they failed to obtain consent for the tracking they performed, and failed to confirm with Hilton
28

1 that its consent procedure was properly implemented. Each of the Third Parties' actions was
2 intentional, and undertaken with willful disregard to their legality, as demonstrated by the fact
3 that they never confirmed that Hilton was properly obtaining consent. The Third Parties had an
4 independent duty to confirm that they had obtained consent, which they breached.

5 144. Because it represented to visitors that they could "opt-out" of cookie tracking for
6 advertising, marketing, and other non-necessary uses, Hilton had a duty to implement the
7 promised opt-out capability. It breached that duty by failing to do so.

8 145. Because Hilton played a significant role in enabling the Third Party's tortious and
9 unlawful conduct (including illegal wiretapping, invasion of privacy, illegal pen register
10 collection, etc.), and it breached its duty to obtain consent and stop collection of data if visitors
11 opted out, it intended to aid and abet the activities of the Third Parties.

12 146. Additionally, on information and belief, Hilton obtained tracking data from the
13 Third Parties for its own use in acquiring new customers, which would have further notified it
14 that data was being collected for all visitors, even those that opted out. This allegation is
15 corroborated by Hilton's 10-Ks, which discuss use of its registration system, Website, and data
16 acquisition as central to its goal of acquiring new customers, as well as retaining loyalty among
17 existing customers.

18 147. Further allegations regarding Hilton's intent and knowledge are incorporated in
19 each cause of action, below.

20 **TOLLING**

21 148. All applicable statutes of limitations have been tolled by operation of the delayed
22 discovery doctrine, which delays accrual until Plaintiffs have, or should have, inquiry notice of
23 their causes of action. Despite exercising reasonable diligence, Plaintiffs were unaware of
24 Defendant's fraudulent and unlawful conduct alleged herein due to Defendant's active
25 concealment of material facts, which prevented Plaintiffs from discovering their claims within
26 the statute of limitations. As alleged above, Plaintiffs do not have the expertise to test whether
27 the Website honored users' requests to opt out of cookies and tracking technologies. Plaintiffs
28

1 were unaware that even though they opted out of cookies on the Website, Defendant caused
2 cookies, including the Third Parties' cookies, to be sent to their browsers, stored on their devices,
3 and transmitted to the Third Parties along with private user data until on or around January 2025
4 when they learned of Defendant's privacy violations from counsel.

5 149. On or around October 14, 2023, Defendant was notified of the claims and
6 allegations asserted herein. Defendant was not prejudiced in its ability to gather evidence for
7 Plaintiffs' claims since the claims asserted herein are substantially similar to those raised in the
8 October 14, 2023 letter.

9 **CLASS ALLEGATIONS**

10 150. Plaintiffs bring this Class Action Complaint on behalf of themselves and a
11 proposed class of similarly situated persons, pursuant to Rules 23(b)(2) and (b)(3) of the Federal
12 Rules of Civil Procedure. Plaintiffs seek to represent the following group of similarly situated
13 persons, defined as follows:

14 **Class:** All persons who browsed the Website in the State of California after clicking the
15 "Opt Out" button in the popup cookies consent banner within the four years preceding
16 the filing of this Complaint (the "Class Period").

17 151. This action has been brought and may properly be maintained as a class action
18 against Defendant because there is a well-defined community of interest in the litigation and the
19 proposed class is easily ascertainable.

20 152. **Numerosity:** Plaintiffs do not know the exact size of the Class, but they estimate
21 that it is composed of more than 100 persons. The persons in the Class are so numerous that the
22 joinder of all such persons is impracticable and the disposition of their claims in a class action
23 rather than in individual actions will benefit the parties and the courts.

24 153. **Common Questions Predominate:** This action involves common questions of
25 law and fact to the Class because each class member's claim derives from the same unlawful
26 conduct that led them to believe that Defendant would not cause third-party cookies to be placed
27 on their browsers and devices and/or transmitted to third parties along with user data, after Class
28

1 members chose to opt out of or reject cookies and tracking technologies on the Website, nor
2 would Defendant permit third parties to track and collect Class members' Private
3 Communications as Class members browsed the Website.

4 154. The common questions of law and fact predominate over individual questions, as
5 proof of a common or single set of facts will establish the right of each member of the Class to
6 recover. The questions of law and fact common to the Class are:

- 7 a. Whether Defendant's actions violate California laws invoked herein; and
8 b. Whether Plaintiffs and Class members are entitled to damages, restitution,
9 injunctive and other equitable relief, reasonable attorneys' fees, prejudgment interest and costs
10 of this suit.

11 155. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of
12 the Class because, among other things, Plaintiffs, like the other Class members, visited the
13 Website, opted out of cookies, and had their confidential Private Communications intercepted
14 by the Third Parties.

15 156. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the
16 interests of all Class members because it is in their best interests to prosecute the claims alleged
17 herein to obtain full compensation due to them for the unfair and illegal conduct of which they
18 complain. Plaintiffs also have no interests in conflict with, or antagonistic to, the interests of
19 Class members. Plaintiffs have retained highly competent and experienced class action attorneys
20 to represent their interests and those of the Class. By prevailing on their claims, Plaintiffs will
21 establish Defendant's liability to all Class members. Plaintiffs and their counsel have the
22 necessary financial resources to adequately and vigorously litigate this class action, and Plaintiffs
23 and counsel are aware of their fiduciary responsibilities to the Class members and are determined
24 to diligently discharge those duties by vigorously seeking the maximum possible recovery for
25 Class members.

26 157. **Superiority:** There is no plain, speedy, or adequate remedy other than by
27 maintenance of this class action. The prosecution of individual remedies by members of the Class
28

will tend to establish inconsistent standards of conduct for Defendant and result in the impairment of Class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the Class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action. Plaintiffs are unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

First Cause of Action: Invasion of Privacy

158. Plaintiffs reallege and incorporate the paragraphs of this Complaint as if set forth herein.

159. To plead a California constitutional privacy claim, Plaintiffs must show an invasion of (i) a legally protected privacy interest; (ii) where Plaintiffs had a reasonable expectation of privacy in the circumstances; and (iii) conduct by Defendant constituting a serious invasion of privacy.

160. Defendant has intruded upon the following legally protected privacy interests of Plaintiffs and Class members: (i) the California Invasion of Privacy Act, as alleged herein; (ii) the California Constitution, which guarantees Californians the right to privacy; (iii) the California Wiretap Acts as alleged herein; (iv) Cal. Penal Code § 484(a), which prohibits the knowing theft or defrauding of property "by any false or fraudulent representation or pretense;" and (v) Plaintiffs' and Class members' Fourth Amendment right to privacy.

161. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as Defendant affirmatively promised users they could "Opt Out" of cookies and

1 tracking technologies before proceeding to browse the Website. Plaintiffs and other Class
2 members directed their electronic devices to access the Website and, when presented with the
3 popup cookies consent banner on the Website, Plaintiffs and Class members opted out of or
4 rejected cookies and reasonably expected that their rejection of cookies and tracking
5 technologies would be honored. That is, they reasonably believed that Defendant would not
6 permit the Third Parties to store and send cookies and/or use other such tracking technologies on
7 their devices while they browsed the Website. Plaintiffs and Class members also reasonably
8 expected that, if they opted out of such cookies and/or tracking technologies, Defendant would
9 not permit the Third Parties to track and collect Plaintiffs' and Class members' Private
10 Communications, including their browsing history, visit history, website interactions, user input
11 data, demographic information, interests and preferences, shopping behaviors, device
12 information, referring URLs, session information, user identifiers, and/or geolocation data, on
13 the Website.

14 162. Such information is "personal information" under California law, which defines
15 personal information as including "Internet or other electronic network activity information,"
16 such as "browsing history, search history, and information regarding a consumer's interaction
17 with an internet website, application, or advertisement." Cal. Civ. Code § 1798.140.

18 163. Defendant, in violation of Plaintiffs' and other Class members' reasonable
19 expectation of privacy and without their consent, permits the Third Parties to use cookies and
20 other tracking technologies to collect, track, and compile users' Private Communications,
21 including their browsing history, visit history, website interactions, user input data, demographic
22 information, interests and preferences, shopping behaviors, device information, referring URLs,
23 session information, user identifiers, and/or geolocation data. The data that Defendant allowed
24 third parties to collect enables the Third Parties to, *inter alia*, create consumer profiles containing
25 detailed information about a consumer's behavior, preferences, and demographics; create
26 audience segments based on shared traits (such as millennials, tech enthusiasts, etc.); and
27 perform targeted advertising and marketing analytics. Further, the Third Parties share user data
28

1 and/or the user profiles to unknown parties to further their financial gain. The consumer profiles
2 are and can be used to further invade Plaintiffs' and users' privacy, by allowing third parties to
3 learn intimate details of their lives, and target them for advertising and other purposes, as
4 described herein, thereby harming them through the abrogation of their autonomy and their
5 ability to control dissemination and use of information about them.

6 164. Defendant's actions constituted a serious invasion of privacy in that it invaded a
7 zone of privacy protected by the Fourth Amendment (i.e., one's personal communications), and
8 violated criminal laws on wiretapping and invasion of privacy. These acts constitute an egregious
9 breach of social norms that is highly offensive. These acts are offensive not only because they
10 involve invasion of personal issue (e.g., travel and movement, relationships, budgets, etc.), but
11 also because they involve breach of an express agreement not to share such information, which
12 is highly offensive on its own.

13 165. Defendant's intrusion into Plaintiffs' privacy was also highly offensive to a
14 reasonable person.

15 166. Defendant lacked a legitimate business interest in causing the placement and/or
16 transmission of third-party cookies along with user data that allowed the Third Parties to track,
17 intercept, receive, and collect Private Communications, including their browsing history, visit
18 history, website interactions, user input data, demographic information, interests and
19 preferences, shopping behaviors, device information, referring URLs, session information, user
20 identifiers, and/or geolocation data, without their consent.

21 167. Plaintiffs and Class members have been damaged by Defendant's invasion of
22 their privacy and are entitled to just compensation, including monetary damages.

23 168. Plaintiffs and Class members seek appropriate relief for that injury, including but
24 not limited to, damages that will compensate them for the harm to their privacy interests as well
25 as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and
26 Class members' privacy.

1 169. Plaintiffs and Class members seek punitive damages because Defendant's
 2 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and
 3 Class members and made in conscious disregard of Plaintiffs' and Class members' rights and
 4 Plaintiffs' and Class members' opt out of the Website's use of cookies. Punitive damages are
 5 warranted to deter Defendant from engaging in future misconduct.

6 **Second Cause of Action: Intrusion Upon Seclusion**

7 170. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

8 171. To assert a claim for intrusion upon seclusion, Plaintiffs must plead (i) that
 9 Defendant intentionally intruded into a place, conversation, or matter as to which Plaintiffs had
 10 a reasonable expectation of privacy; and (ii) that the intrusion was highly offensive to a
 11 reasonable person.

12 172. By permitting third-party cookies to be stored on consumers' devices, which
 13 enabled the Third Parties to track and collect Plaintiffs' and Class members' Private
 14 Communications, including their browsing history, visit history, website interactions, user input
 15 data, demographic information, interests and preferences, shopping behaviors, device
 16 information, referring URLs, session information, user identifiers, and/or geolocation data, in
 17 violation of Defendant's representations otherwise in the popup cookie consent banner,
 18 Defendant intentionally intruded upon the solitude or seclusion of Website users. Defendant
 19 effectively placed the Third Parties in the middle of communications to which they were not
 20 invited, welcomed, or authorized.

21 173. The Third Parties' tracking and collecting of Plaintiffs' and Class member's
 22 Private Communications on the Website using third-party cookies that Defendant caused to be
 23 stored on users' devices—and to be transmitted to Third Parties—was not authorized by
 24 Plaintiffs and Class members, and, in fact, those Website users specifically chose to "Opt Out"
 25 of cookies.

26 174. Plaintiffs and the Class members had an objectively reasonable expectation of
 27 privacy surrounding their Private Communications on the Website based on Defendant's
 28

1 promise that users could “Opt Out” of cookies, as well as state criminal and civil laws designed
2 to protect individual privacy.

3 175. Defendant’s intentional intrusion into Plaintiffs’ and other users’ Private
4 Communications would be highly offensive to a reasonable person given that Defendant
5 represented that Website users could “Opt Out” of cookies when, in fact, Defendant caused such
6 third-party cookies to be stored on consumers’ devices and browsers, and to be transmitted to
7 third parties, even when consumers opted out of or rejected all such cookies. Indeed, Plaintiffs
8 and Class members reasonably expected, based on Defendant’s false representations, that when
9 they opted out of cookies and tracking technologies, Defendant would not cause such third-party
10 cookies to be stored on their devices or permit the Third Parties to obtain their Private
11 Communications on the Website, including their browsing history, visit history, website
12 interactions, user input data, demographic information, interests and preferences, shopping
13 behaviors, device information, referring URLs, session information, user identifiers, and/or
14 geolocation data.

15 176. Defendant’s conduct was intentional and intruded on Plaintiffs’ and users’ Private
16 Communications on the Website. These acts are offensive not only because they involve
17 intrusion into personal issues (e.g., travel and movement, relationships, budgets, etc.), but also
18 because they involve breach of an express promise not to share such information, which is highly
19 offensive on its own.

20 177. Plaintiffs and Class members have been damaged by Defendant’s invasion of
21 their privacy and are entitled to just compensation, including monetary damages.

22 178. Plaintiffs and Class members seeks appropriate relief for that injury, including
23 but not limited to, damages that will compensate them for the harm to their privacy interests as
24 well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs’
25 and Class members’ privacy.

26 179. Plaintiffs and Class members seek punitive damages because Defendant’s
27 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and
28

Class members and made in conscious disregard of Plaintiffs’ and Class members’ rights and Plaintiffs’ and Class members’ opt out of and rejection of the Website’s use of cookies. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

Third Cause of Action: Wiretapping in Violation of the California Invasion of Privacy Act (California Penal Code § 631)

180. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

181. California Penal Code § 631(a) provides, in pertinent part:

“Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars”

182. The California Supreme Court has repeatedly stated an “express objective” of CIPA is to “protect a person placing or receiving a call from a situation where the person on the other end of the line permits an outsider to tap his telephone or listen in on the call.” *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

183. Further, as the California Supreme Court has held, in explaining the legislative purpose behind CIPA:

While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and *its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device*.

As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas, 38 Cal. 3d at 360-61 (emphasis supplied; internal citations omitted).

184. CIPA § 631(a) imposes liability for “distinct and mutually independent patterns of conduct.” *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability

under § 631(a), Plaintiffs need only establish that Defendant, “by means of any machine, instrument, contrivance, or in any other manner,” did *any* of the following:

[i] Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;

[ii] Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

[iii] Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained

Cal. Penal Code § 631(a).

185. CIPA § 631(a) also penalizes those who [iv] “aid[], agree[] with, employ[], or conspire[] with any person” who conducts the aforementioned wiretapping, or those who “permit” the wiretapping.

186. Defendant is a “person” within the meaning of California Penal Code § 631.

187. Section 631(a) is not limited to phone lines, but also applies to “new technologies” such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic communications”); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping, Section 631(a) applies to Internet communications.”).

188. The Third Parties’ cookies—as well as the software code of the Third Parties responsible for placing the cookies and transmitting data from user devices to the Third Parties—constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA (and, even if they do not, Defendant’s deliberate and purposeful scheme that facilitated the interceptions falls under the broad statutory catch-all category of “any other manner”).

1 189. Each of the Third Parties is a “separate legal entity that offers [a] ‘software-as-a-
2 service’ and not merely a passive device.” *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D.
3 Cal. 2021). Further, the Third Parties had the capability to use the wiretapped information for
4 their own purposes and, as alleged above, they did in fact use the wiretapped information for their
5 own business purposes. Accordingly, the Third Parties were third parties to any communication
6 between Plaintiffs and Class members, on the one hand, and Defendant, on the other. *Id.* at 521;
7 see also *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

8 190. Under § 631(a), Defendant must show it had the consent of all parties to a
9 communication.

10 191. At all relevant times, the Website caused Plaintiffs’ and Class members’ browsers
11 to store the Third Parties’ cookies and to transmit those cookies—including their browsing
12 history, visit history, website interactions, user input data, demographic information, interests and
13 preferences, shopping behaviors, device information, referring URLs, session information, user
14 identifiers, and/or geolocation data—alongside Private Communications (including location
15 search strings, proposed dates of visits, number of people, and other selection data input by
16 Plaintiffs and Class members and communicated to Defendant) to the Third Parties without
17 Plaintiffs’ and Class members’ consent. By configuring the Website in this manner, Defendant
18 willfully aided, agreed with, employed, permitted, or otherwise enabled the Third Parties to
19 wiretap Plaintiffs and Class members using the Third Parties’ cookies and to accomplish the
20 wrongful conduct alleged herein.

21 192. At all relevant times, by their cookies and corresponding software code, the Third
22 Parties willfully and without the consent of all parties to the communication, or in any
23 unauthorized manner, read, attempted to read, and/or learned the contents or meaning of
24 electronic communications of Plaintiffs and Class members, on the one hand, and Defendant, on
25 the other, while the electronic communications were in transit or were being sent from or received
26 at any place within California.

1 193. The Private Communications of Plaintiffs and Class members, on the one hand,
2 and Defendant, on the other, that the Third Parties automatically intercepted directly
3 communicates the Website user's affirmative decisions, actions, choices, preferences, and
4 activities, which constitute the "contents" of electronic communications, including their browsing
5 history, visit history, website interactions, user input data, demographic information, interests and
6 preferences, shopping behaviors, device information, referring URLs, session information, user
7 identifiers, and/or geolocation data.

8 194. At all relevant times, the Third Parties used or attempted to use the Private
9 Communications automatically intercepted by their cookie tracking technologies for their own
10 purposes.

11 195. Plaintiffs and Class members did not provide their prior consent to the Third
12 Parties' intentional access, interception, reading, learning, recording, collection, and usage of
13 Plaintiffs' and Class members' electronic communications. Nor did Plaintiffs and Class members
14 provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or
15 otherwise enabling the Third Parties' conduct. On the contrary, Plaintiffs and Class members
16 expressly declined to allow Third Parties' cookies and tracking technologies to access, intercept,
17 read, learn, record, collect, and use Plaintiffs' and Class members' electronic communications by
18 choosing to opt out of cookies in the consent banner.

19 196. The wiretapping of Plaintiffs and Class members occurred in California, where
20 Plaintiffs and Class members accessed the Website and where the Third Parties—as enabled by
21 Defendant—routed Plaintiffs' and Class members' electronic communications to Third Parties'
22 servers. Among other things, the cookies, as well as the software code responsible for placing the
23 cookies and transmitting them and other Private Communications to the Third Parties, resided on
24 Plaintiffs' California-located devices. In particular, the user's California-based device, after
25 downloading the software code from the Third Parties' servers, (i) stored the code onto the user's
26 disk; (ii) converted the code into machine-executable format; and (iii) executed the code, causing
27 the transmission of data (including cookie data) to and from the Third Parties.

197. Plaintiffs and Class members have suffered loss by reason of these violations, including, but not limited to, (i) violation of their right to privacy; (ii) loss of value in their Private Communications; (iii) damage to and loss of Plaintiff's and Class members' property right to control the dissemination and use of their Private Communications; and (iv) loss of their Private Communications to the Third Parties with no consent.

198. Pursuant to California Penal Code § 637.2, Plaintiffs and Class members have been injured by the violations of California Penal Code § 631, and each seeks statutory damages of the greater of \$5,000, or three times the amount of actual damages, for each of Defendant's violations of CIPA § 631(a), as well as injunctive relief.

199. Unless enjoined, Defendant will continue to commit the illegal acts alleged herein including, but not limited to, permitting third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Plaintiffs, Class members, and the general public continue to be at risk because Plaintiffs, Class members, and the general public frequently use the internet to search for information and content related to its hotels and resorts. Plaintiffs, Class members, and the general public continue to desire to use the internet for that purpose. Plaintiffs, Class members, and the general public have no practical way to know if their request to opt out of cookies and tracking technologies will be honored and/or whether Defendant will permit third parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant. Further, Defendant has already permitted the Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class members' electronic Private Communications with Defendant and will continue to do so unless and until enjoined.

Fourth Cause of Action: Use of a Pen Register in Violation of the California Invasion of Privacy Act (California Penal Code § 638.51)

200. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

201. The California Invasion of Privacy Act, codified at Cal. Penal Code §§ 630 to 638, includes the following statement of purpose:

The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of

1 eavesdropping upon private communications and that the invasion of privacy
2 resulting from the continual and increasing use of such devices and techniques
has created a serious threat to the free exercise of personal liberties and cannot be
tolerated in a free and civilized society.

3 202. California Penal Code Section 638.51(a) proscribes any “person” from
4 “install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court
5 order.”

6 203. A “pen register” is a “a device or process that records or decodes dialing, routing,
7 addressing, or signaling information transmitted by an instrument or facility from which a wire
8 or electronic communication is transmitted, but not the contents of a communication.” Cal. Penal
9 Code § 638.50(b).

10 204. The Third Parties’ cookies and the corresponding software code installed by
11 Defendant on its Website are each “pen registers” because they are “device[s] or process[es]”
12 that “capture[d]” the “routing, addressing, or signaling information”—including, the IP address
13 and user-agent information—from the electronic communications transmitted by Plaintiffs’ and
14 the Class’s computers or devices. Cal. Penal Code § 638.50(b).

15 205. At all relevant times, Defendant caused the Third Parties’ cookies and the
16 corresponding software code—which are pen registers—to be placed on Plaintiffs’ and Class
17 members’ browsers and devices, and/or to be used to transmit Plaintiffs’ and Class members’ IP
18 address and user-agent information. *See Greenley v. Kochava*, 2023 WL 4833466, at *15-16
19 (S.D. Cal. July 27, 2023); *Shah v. Fandom, Inc.*, 2024 U.S. Dist. LEXIS 193032, at *5-11 (N.D.
20 Cal. Oct. 21, 2024).

21 206. Some of the information collected by the Third Parties’ cookies and the
22 corresponding software, including IP addresses, device identifiers, and user-agent information,
23 does not constitute the content of Plaintiffs’ and the Class’s electronic communications with the
24 Website. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1008 (9th Cir. 2014). (“IP addresses
25 constitute addressing information and do not necessarily reveal any more about the underlying
26 contents of communication...”)(cleaned up).

1 207. Plaintiffs and Class members did not provide their prior consent to Defendant's
2 use of third-party cookies and the corresponding software. On the contrary, Plaintiffs and the
3 Class members informed Defendant that they did not consent to the Website's use of third-party
4 cookies by clicking the "Opt Out" button in the cookie consent banner.

5 208. Defendant did not obtain a court order to install or use the third-party cookies and
6 the corresponding software to track and collect Plaintiffs' and Class member's IP addresses and
7 user-agent information.

8 209. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class
9 members suffered losses and were damaged in an amount to be determined at trial.

10 210. Pursuant to Penal Code § 637.2(a)(1), Plaintiffs and Class members are also
11 entitled to statutory damages of \$5,000 for each of Defendant's violations of § 638.51(a).

12 **Fifth Cause of Action: Common Law Fraud, Deceit and/or Misrepresentation**

13 211. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

14 212. Defendant fraudulently and deceptively informed Plaintiffs and Class members
15 that they could "Opt Out" of cookies.

16 213. However, despite Defendant's representations otherwise, Defendant caused third-
17 party cookies and software code to be stored on consumers' devices, and to be transmitted to the
18 Third Parties alongside Private Communications, even after users clicked the "Opt Out" button
19 in the popup cookie consent banner. These cookies and corresponding software code allowed the
20 Third Parties to access, intercept, read, learn, record, collect, and use Plaintiffs' and Class
21 members' Private Communications, even when consumers had previously chosen to "Opt Out"
22 of cookies.

23 214. These misrepresentations and omissions were known exclusively to, and actively
24 concealed by Defendant, not reasonably known to Plaintiffs and Class members, and material at
25 the time they were made. Defendant knew, or should have known, how the Website functioned,
26 including the Third Party's resources it installed on the Website and the third-party cookies in
27 use on the Website, through testing the Website, evaluating its performance metrics by means of
28

1 its accounts with the Third Parties, or otherwise, and knew, or should have known, that the
2 Website’s programming allowed the third-party cookies to be placed on users’—including
3 Plaintiffs’—browsers and devices and/or transmitted to the Third Parties along with users’
4 Private Communications even after users attempted to “Opt Out” of cookies, which Defendant
5 promised its users they could do. Defendant’s misrepresentations and omissions concerned
6 material facts that were essential to the analysis undertaken by Plaintiffs and Class members as
7 to whether to use the Website. In misleading Plaintiffs and Class members and not so informing
8 them, Defendant breached its duty to Plaintiffs and Class members. Defendant also gained
9 financially from, and as a result of, its breach.

10 215. Plaintiffs and Class members relied to their detriment on Defendant’s
11 misrepresentations and fraudulent omissions.

12 216. Plaintiffs and Class members have suffered an injury-in-fact, including the loss
13 of money and/or property, as a result of Defendant’s unfair, deceptive, and/or unlawful practices,
14 including the unauthorized interception of their Personal Communications, including their
15 browsing history, visit history, website interactions, user input data, demographic information,
16 interests and preferences, shopping behaviors, device information, referring URLs, session
17 information, user identifiers, and/or geolocation data, which have value as demonstrated by the
18 use and sale of consumers’ browsing activity, as alleged above. Plaintiffs and Class members
19 have also suffered harm in the form of diminution of the value of their private and personally
20 identifiable information and communications.

21 217. Defendant’s actions caused damage to and loss of Plaintiffs’ and Class members’
22 property right to control the dissemination and use of their personal information and
23 communications.

24 218. Defendant’s representation that consumers could opt out of cookies (including
25 “cookies and similar technologies to provide you with personalized content, improve site
26 performance, and conduct analytics ... [and] advertisements”) if they clicked the “Opt Out”
27 button was untrue. Again, had Plaintiffs and Class members known these facts, they would not
28

1 have used the Website. Moreover, Plaintiffs and Class members reviewed the popup cookie
2 consent banner and Privacy Statement prior to their interactions with the Website. Had
3 Defendant disclosed that it caused third-party cookies to be stored on Website visitors' devices
4 that are related to personalization, advertising, and analytics and/or share information with third
5 parties even after they choose to opt out of all such cookies, Plaintiffs and Class members would
6 have noticed it and would not have interacted with the Website.

7 219. By and through such fraud, deceit, misrepresentations and/or omissions,
8 Defendant intended to induce Plaintiffs and Class members to alter their positions to their
9 detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiffs and Class
10 members to, without limitation, use the Website under the mistaken belief that Defendant would
11 not permit third parties to obtain users' Private Communications when consumers chose to opt
12 out of cookies. As a result, Plaintiff and the Class provided more personal data than they would
13 have otherwise.

14 220. Plaintiffs and Class members justifiably and reasonably relied on Defendant's
15 misrepresentations and omissions, and, accordingly, were damaged by Defendant's conduct.

16 221. As a direct and proximate result of Defendant's misrepresentations and/or
17 omissions, Plaintiffs and Class members have suffered damages, as alleged above, and are
18 entitled to just compensation, including monetary damages.

19 222. Plaintiffs and Class members seek punitive damages because Defendant's
20 actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and
21 Class members and made in conscious disregard of Plaintiffs' and Class members' rights and
22 Plaintiffs' and Class members' opt out of and rejection of the Website's use of cookies. Punitive
23 damages are warranted to deter Defendant from engaging in future misconduct.

24 **Sixth Cause of Action: Unjust Enrichment**

25 223. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

26 224. Defendant created and implemented a scheme to increase its own profits through
27 a pervasive pattern of false statements and fraudulent omissions.
28

1 225. Defendant was unjustly enriched as a result of its wrongful conduct, including
2 through its misrepresentation that users could “Opt Out” of cookies and by permitting the Third
3 Parties to store and transmit cookies on Plaintiffs’ and Class members’ devices and browsers,
4 which permitted the Third Parties to track and collect users’ Private Communications, including
5 their browsing history, visit history, website interactions, user input data, demographic
6 information, interests and preferences, shopping behaviors, device information, referring URLs,
7 session information, user identifiers, and/or geolocation data, even after Class members opted
8 out of such cookies.

9 226. Plaintiffs and Class members’ Personal Communications have conferred an
10 economic benefit on Defendant.

11 227. Defendant has been unjustly enriched at the expense of Plaintiffs and Class
12 members, and Defendant has unjustly retained the benefits of its unlawful and wrongful conduct.

13 228. Defendant appreciated, recognized, and chose to accept the monetary benefits that
14 Plaintiffs and Class members conferred onto Defendant at their detriment. These benefits were
15 the expected result of Defendant acting in its pecuniary interest at the expense of Plaintiffs and
16 Class members.

17 229. It would be unjust for Defendant to retain the value of Plaintiffs’ and Class
18 members’ property and any profits earned thereon.

19 230. There is no justification for Defendant’s enrichment. It would be inequitable,
20 unconscionable, and unjust for Defendant to be permitted to retain these benefits because the
21 benefits were procured as a result of its wrongful conduct.

22 231. Plaintiffs and Class members are entitled to restitution of the benefits Defendant
23 unjustly retained and/or any amounts necessary to return Plaintiffs and Class members to the
24 position they occupied prior to having their Private Communications tracked and collected by
25 the Third Parties.

26 232. Plaintiffs plead this claim separately, as well as in the alternative, to their other
27 claims, as without such claims Plaintiffs would have no adequate legal remedy.
28

Seventh Cause of Action: Breach of Contract

233. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

234. Defendant's relationship with its users is governed by the Website's Privacy Statement, which explains:

Hilton's mission is to be the most hospitable company in the world. We're passionate about delivering exceptional guest experiences, and we look forward to welcoming you to our hotels so we can share the light and warmth of hospitality with you.

We pledge to deliver the highest level of customer service, which includes respecting your privacy and protecting your personal information. In this privacy statement ("Statement"), we provide you with details about how we collect, use, and disclose your personal information.

This Statement applies to Hilton Worldwide Holdings Inc., its subsidiaries, and all of the hotels within the Hilton Portfolio of Brands (collectively, "Hilton," "we," or "us"). Our Portfolio of Brands includes Waldorf Astoria Hotels & Resorts, LXR Hotels & Resorts, Conrad Hotels & Resorts, Canopy by Hilton, Signia by Hilton, Hilton Hotels & Resorts, Curio Collection by Hilton, DoubleTree by Hilton, Tapestry Collection by Hilton, Embassy Suites by Hilton, Tempo by Hilton, Motto by Hilton, Hilton Garden Inn, Hampton by Hilton, Tru by Hilton, Homewood Suites by Hilton, and Home2 Suites by Hilton.

By using any of our products or services and/or by agreeing to this Statement, e.g. in the context of registering for any of our products or services, you understand and acknowledge that we will collect and use personal information as described in this Statement.

235. The Website's Privacy Statement contains enforceable promises that Defendant made to Plaintiffs and Class members, including, but not limited to, the following provision:

If you would like to opt out of the sale of your personal information, you may do so by clicking on the banner that appears on any Hilton website when you access that site from an IP address that relates to California or by visiting our website at datarights.hilton.com or click the "Personal Data Requests" link at the bottom of any Hilton website to submit your request. Please note that when you opt out of cookies, tags, and pixels, that opt out only pertains to the device and the browser that you are using when you opt out. If you wish to opt out for other devices or browsers, you must opt out again when you are using those devices or browsers.

236. Defendant breached these duties and violated these promises by causing third-party cookies to be stored on consumers' devices and browsers that enabled the Third Parties to track and collect Plaintiffs' and Class member's Private Communications, including their

browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even though Defendant represented that Plaintiffs and other users could “Opt Out” of cookies. Plaintiffs and Class members, in fact, chose to opt out of such cookies by selecting the “Opt Out” button.

237. At all relevant times and in all relevant ways, Plaintiffs and Class members performed their obligations under the Privacy Statement or were excused from performance of such obligations through the unknown and unforeseen conduct of others.

238. Defendant’s conduct in permitting the Third Parties to track and collect the Private Communications of Website users who chose to reject all cookies and tracking technologies evaded the spirit of the bargain made between Defendant and Plaintiff and Class members since it caused Plaintiff and Class members to surrender more data than they had otherwise bargained for.

239. As a direct and proximate result of Defendant’s breach of contract, Plaintiffs and Class members did not receive the full benefit of the bargain, and instead received services from Defendant that were less valuable than described in the Privacy Statement. Plaintiffs and Class members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendant’s partial, deficient, and/or defective performance.

240. As a direct consequence of the breaches of contract and violations of promises described above, Plaintiffs and Class members seek nominal damages, general damages, compensatory damages, consequential damages, unjust enrichment, and any other just relief.

Eighth Cause of Action: Breach of Implied Covenant of Good Faith and Fair Dealing

241. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

242. Defendant’s relationship with its users is governed by the Website’s Privacy Statement, which explains:

Hilton’s mission is to be the most hospitable company in the world. We’re passionate about delivering exceptional guest experiences, and we look forward to welcoming you to our hotels so we can share the light and warmth of hospitality with you.

1 We pledge to deliver the highest level of customer service, which includes
2 respecting your privacy and protecting your personal information. In this
3 privacy statement (“Statement”), we provide you with details about how we
collect, use, and disclose your personal information.

4 This Statement applies to Hilton Worldwide Holdings Inc., its subsidiaries, and
5 all of the hotels within the Hilton Portfolio of Brands (collectively, “Hilton,”
6 “we,” or “us”). Our Portfolio of Brands includes Waldorf Astoria Hotels &
7 Resorts, LXR Hotels & Resorts, Conrad Hotels & Resorts, Canopy by Hilton,
8 Signia by Hilton, Hilton Hotels & Resorts, Curio Collection by Hilton,
9 DoubleTree by Hilton, Tapestry Collection by Hilton, Embassy Suites by
Hilton, Tempo by Hilton, Motto by Hilton, Hilton Garden Inn, Hampton by
Hilton, Tru by Hilton, Homewood Suites by Hilton, and Home2 Suites by
Hilton.

10 By using any of our products or services and/or by agreeing to this Statement,
11 e.g. in the context of registering for any of our products or services, you
12 understand and acknowledge that we will collect and use personal information
as described in this Statement.

13 243. The Website’s Privacy Statement contains enforceable promises that Defendant
14 made to Plaintiffs and Class members, including, but not limited to, the following provision:

15 If you would like to opt out of the sale of your personal information, you may do
16 so by clicking on the banner that appears on any Hilton website when you access
17 that site from an IP address that relates to California or by visiting our website at
18 datarights.hilton.com or click the “Personal Data Requests” link at the bottom of
19 any Hilton website to submit your request. Please note that when you opt out of
cookies, tags, and pixels, that opt out only pertains to the device and the browser
that you are using when you opt out. If you wish to opt out for other devices or
browsers, you must opt out again when you are using those devices or browsers.

20 244. Defendant breached these duties and violated these promises by causing third-
21 party cookies to be stored on consumers’ devices and browsers that enabled the Third Parties to
22 track and collect Plaintiffs’ and Class member’s Private Communications, including their
23 browsing history, visit history, website interactions, user input data, demographic information,
24 interests and preferences, shopping behaviors, device information, referring URLs, session
25 information, user identifiers, and/or geolocation data, even though Defendant represented that
26 Plaintiffs and other users could opt out of cookies and tracking technologies. Plaintiffs and Class
27 members, in fact, chose to opt out of such cookies by selecting the “Opt Out” button. California
28 law recognizes the implied covenant of good faith and fair dealing in every contract.

1 245. In dealing between Defendant and its Website users, Defendant is invested with
2 discretionary power affecting the rights of its users.

3 246. Defendant purports to respect and protect its Website users' privacy.

4 247. Despite their contractual promises to allow consumers to opt out of cookies and
5 other tracking technologies, Defendant took actions outside that contractual promise to deprive
6 consumers, including Plaintiffs and other users similarly situated, of benefits of their contract
7 with Defendant.

8 248. Defendant's allowance of third parties to track and collect Website users' Private
9 Communications with Defendant was objectively unreasonable given its privacy promises.

10 249. Defendant's conduct in permitting third parties to track and collect the Private
11 Communications of Website users who chose to opt out of cookies and tracking technologies
12 evaded the spirit of the bargain made between Defendant and Plaintiffs and Class members since
13 it caused Plaintiffs and Class members to surrender more data than they had otherwise bargained
14 for.

15 250. As a result of Defendant's misconduct and breach of its duty of good faith and
16 fair dealing, Plaintiffs and Class members suffered damages. Plaintiffs and Class members did
17 not receive the benefit of the bargain for which they contracted and for which they paid valuable
18 consideration in the form of providing their personal information, which, as alleged above, has
19 ascertainable value.

20 251. As a direct consequence of the breach of the implied covenant of good faith and
21 fair dealing described above, Plaintiffs and Class members seek nominal damages, general
22 damages, compensatory damages, consequential damages, and any other just relief.

23 **Ninth Cause of Action: Trespass to Chattels**

24 252. Plaintiffs reallege and incorporate by reference all paragraphs alleged herein.

25 253. Defendant, intentionally and without consent or other legal justification, caused
26 cookies to be stored on Plaintiffs' and Class members' browsers and devices, which enabled the
27
28

1 Third Parties and Defendant to track and collect Plaintiffs' and Class members' Private
2 Communications and use the data collected for their own advantage, as described above.

3 254. Defendant was unjustly enriched as a result of its wrongful conduct, including
4 through its misrepresentation that users could opt out of cookies and tracking technologies, and
5 through their failure to disclose that Defendant causes third-party cookies to be stored on
6 consumers' devices and browsers, which cause the Third Parties and Defendant to track and
7 collect Plaintiffs' and Class members' Private Communications even after consumers chose to
8 opt out of or reject such cookies.

9 255. Defendant intentionally caused third party software code to be stored onto
10 Plaintiffs' and Class members' devices, knowing that the code would be executed by those
11 devices. The software code then placed and/or transmitted cookies along with Plaintiffs' and
12 Class members' Private Communications to the Third Parties. These intentional acts interfered
13 with Plaintiffs' and Class members' use of the following personal property owned, leased, or
14 controlled by Plaintiffs and other users: (a) her and their computers and other electronic devices;
15 and (b) her and their personally identifiable information.

16 256. Defendant's trespass of Plaintiffs' and other users' computing devices resulted in
17 harm to Plaintiffs and other users and caused Plaintiffs and other users the following damages:

- 18 a. Nominal damages for trespass;
19 b. Reduction of storage, disk space, and performance of Plaintiffs' and Class
20 members' computing devices; and
21 c. Loss of value of Plaintiffs' and Class members' computing devices.

22 **PRAYER FOR RELIEF**

23 **WHEREFORE**, reserving all rights, Plaintiffs, on behalf of themselves and the Class
24 members, respectfully request judgment against Defendant as follows:

25 A. Certification of the proposed Class, including appointment of Plaintiffs' counsel
26 as class counsel;
27
28

1 B. An award of compensatory damages, including statutory damages where
2 available, to Plaintiffs and Class members against Defendant for all damages sustained as a result
3 of Defendant's wrongdoing, including both pre- and post-judgment interest thereon;

4 C. An award of punitive damages;

5 D. An award of nominal damages;

6 E. An order for full restitution;

7 F. An order requiring Defendant to disgorge revenues and profits wrongfully
8 obtained;

9 G. An order temporarily and permanently enjoining Defendant from continuing the
10 unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

11 H. For reasonable attorneys' fees and the costs of suit incurred; and

12 I. For such further relief as may be just and proper.
13

14 Dated: June 25, 2025

GUTRIDE SAFIER LLP

/s/ Anthony J. Patek

Seth A. Safier (State Bar No. 197427)

seth@gutridesafier.com

Marie A. McCrary (State Bar No. 262670)

marie@gutridesafier.com

Todd Kennedy (State Bar No. 250267)

todd@gutridesafier.com

Kali R. Backer (State Bar No. 342492)

kali@gutridesafier.com

Anthony J. Patek (State Bar No. 228964)

anthony@gutridesafier.com

100 Pine Street, Suite 1250

San Francisco, CA 94111

Telephone: (415) 639-9090

Facsimile: (415) 449-6469

Attorneys for Plaintiff